

**UNIVERSIDADE FEDERAL DO RIO DE JANEIRO**  
**CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS**  
**FACULDADE DE DIREITO**

**O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS E O  
DIREITO DE ACESSO NA LGPD (LEI 13.709/18)**

**MIGUEL PEDRO ALVES DA PAZ**

**RIO DE JANEIRO – RJ**  
**PLE 1/2020**

**MIGUEL PEDRO ALVES DA PAZ**

**O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS E O  
DIREITO DE ACESSO NA LGPD (LEI 13.709/18)**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Magalhães Martins.**

**RIO DE JANEIRO – RJ**

**PLE 1/2020**

### CIP - Catalogação na Publicação

PP348d Paz, Miguel Pedro Alves da  
O desenvolvimento do Direito à Proteção de Dados  
Pessoais e o Direito de Acesso na LGPD (Lei  
13.709/18) / Miguel Pedro Alves da Paz. -- Rio de  
Janeiro, 2020.  
76 f.

Orientador: Guilherme Magalhães Martins.  
Trabalho de conclusão de curso (graduação) -  
Universidade Federal do Rio de Janeiro, Faculdade  
Nacional de Direito, Bacharel em Direito, 2020.

1. Proteção de Dados Pessoais. 2. Autodeterminação  
Informativa. 3. Tratamento de Dados. 4. Lei Geral  
de Proteção de Dados. 5. Direito de Acesso. I.  
Martins, Guilherme Magalhães, orient. II. Título.

**MIGUEL PEDRO ALVES DA PAZ**

**O DESENVOLVIMENTO DO DIREITO À PROTEÇÃO DE DADOS PESSOAIS E O  
DIREITO DE ACESSO NA LGPD (LEI 13.709/18)**

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do **Professor Dr. Guilherme Magalhães Martins.**

Data da Aprovação: 13/11/2020.

Banca Examinadora:

**GUILHERME MAGALHÃES MARTINS**  
Orientador

**ANDREIA FERNANDES DE ALMEIDA RANGEL**  
Membro da Banca

**JULIANA DE SOUSA GOMES LAGE**  
Membro da Banca

**RIO DE JANEIRO – RJ**

**PLE 1/2020**

Aos meus pais, Marcio e Fernanda, pela formação contínua em minha vida.

À minha irmã, Micaela, pela companhia na jornada.

À Bruna, pelo amor e dedicação.

A Deus, que preenche meu coração e me chama a servir ao outro  
através das minhas capacidades.

## **AGRADECIMENTOS**

Em primeiro lugar, a Deus, que em sua infinita bondade me sustenta e a cada dia realiza maravilhas em minha vida nas grandes e pequenas coisas, pois sua misericórdia é infinita e seu amor é fiel. Também à Virgem Maria, minha advogada, que me ampara e intercede por mim sem largar a minha mão.

Aos meus pais, Marcio e Fernanda, que sempre me incentivaram e me possibilitaram chegar até aqui. Foi através de sua entrega que alcancei tudo em minha vida, e por sua dedicação em me formar em todos os âmbitos e em todos os momentos eu me tornei quem sou.

À minha irmã, Micaela, importante companhia desde sempre, é uma das maiores ligações que tenho na vida. Obrigado pelas ajudas técnicas e pelas ótimas refeições e cafés que fizeram diferença na tensão da rotina, especialmente neste momento pandêmico.

À Bruna, meu amor, que me impulsionou e com quem mais compartilhei as dores nesses anos de faculdade. Obrigado por sua paciência para conhecer minha versão estendida, pela presença e pelo carinho. A confiança que deposita em mim me motiva e me faz caminhar rumo a minha melhor versão.

Aos meus avós, José e Lucinha, por toda a preocupação, júbilo e carinho manifestado em gestos que fizeram grande diferença nessa jornada. Aos meus sogros, Flavio e Rosinha, e meu cunhado, Hugo, por todo o incentivo e credibilidade durante esse tempo.

A tantos amigos que foram presentes (mesmo que à distância) na caminhada até aqui. Às companhias de ônibus, às caronas, e em especial aqueles que comigo enfrentaram as batalhas da graduação e que guardarei para a vida: Lucas Vale, Ivantuil Franchini, Diogo Costa, Cátia Araujo, Elaine Vieira, Daniele Inês, Clarissa Mendes, Vinicius Rezende e Leonardo Vieira. Vocês fizeram a faculdade se tornar um tempo muito mais proveitoso e vencer cada luta ao lado de vocês mostrava que Deus sempre está do nosso lado através dos amigos. Vencemos!

Aos professores com quem tive a honra de aprender tanto sobre as disciplinas quanto sobre a vida, em especial Cintia Konder, Eduardo Moreira, Cesar Augusto, Ubirajara Neto, Chiara de Teffé, Maici Barbosa e Guilherme Martins.

Ao professor Allan Turano minha gratidão pelo pequeno gesto de incentivar a escrever um artigo para uma disciplina e, através deste, proporcionar um enorme crescimento em minha formação, com uma monitoria e disciplina inéditas na Faculdade Nacional de Direito e material escrito para fora da universidade. Obrigado por todo o apoio, exemplo e pelas oportunidades de desenvolvimento.

Aos meus colegas de trabalho de ontem e de hoje, em especial, Rafael, Sylvia, Paula, Livia, Vanise, Leonardo, Daniel, Daniele, Diogo, Iago, Isadora, Carol e Guilherme, que contribuíram direta ou indiretamente neste resultado, pelos incentivos, pelo que pude aprender com vocês e pelo ambiente que, em cada tempo, foi importante para meu desenvolvimento como profissional e pessoa, além, é claro, das caronas que facilitavam a vida do universitário da baixada fluminense que estudava na capital.

Por fim, a todos os que contribuíram com orações, com conversas e, até mesmo sem saber, com sorrisos e pequenas gestos que me fortaleciam na luta de cada dia. Foi uma longa jornada, com muitas escolhas, muitos obstáculos, mas também com muito crescimento, felicidade e descobertas que me fizeram admirar ainda mais a vida e as possibilidades que temos a cada momento.

Termino esta etapa ciente de que a vida e as nossas oportunidades são muito melhor aproveitadas quando compartilhadas com quem amamos. Saber observar cada possibilidade de crescimento nas relações com as pessoas que nos rodeiam é uma virtude que quero conquistar a cada dia. Que venham as próximas jornadas e fases e que eu permaneça sempre com um sorriso para quem comigo encontrar.

“O homem é livre porque possui a faculdade de se determinar em função da verdade e do bem. O homem é livre porque possui a faculdade de escolher movido e determinado por uma convicção pessoal interior, e não simplesmente por efeito de impulsos instintivos cegos ou por mera coação externa. Ser livre é poder e querer escolher, é viver segundo a própria consciência.”

(Karol Wojtyła)



## **RESUMO**

A presente monografia tem por objetivo estudar a normatização do direito à proteção de dados pessoais e sua capacidade de tutelar o ser humano, garantindo aos indivíduos maior liberdade para desenvolver sua personalidade dentro da sociedade. Para tanto, analisa-se inicialmente o desenvolvimento do direito à proteção de dados no mundo ao longo dos anos. Avança-se para uma pesquisa sobre a garantia desse direito no ordenamento jurídico brasileiro através de normativas dispersas até a chegada da Lei Geral de Proteção de Dados, num processo de fortalecimento da proteção à pessoa e da segurança jurídica ligadas às atividades que processam dados pessoais. Termina-se analisando a relevância do direito de acesso na proteção dos dados, como este foi concebido na LGPD, a sua abrangência, a forma como deve ser assegurado, quais as consequências práticas de se garantir tal direito ao titular e o que pode contribuir para a sua efetivação.

Palavras-chave: Proteção de Dados Pessoais; Autodeterminação Informativa; Tratamento de Dados, Lei Geral de Proteção de Dados; Direito de Acesso

## **ABSTRACT**

This monograph aims to study the regulation of personal data protection and its ability to protect human beings, guaranteeing individuals greater freedom to develop their personality within society. In order to do so, the development of the right to data protection in the world over the years is analyzed. Following, research on the guarantee of this right in the Brazilian legal system through scattered norms until the arrival of the General Data Protection Law, in a process of strengthening the protection of the person and legal security related to the activities of personal data processing. It ends by analyzing the relevance of the right of access for the data protection, how it was conceived in the GPDL, its scope, how it should be ensured, what are the practical consequences of guaranteeing such a right to the holder, and what can contribute to its effectiveness.

**Keywords:** Personal Data Protection; Informational self-determination; Data Processing; General Data Protection Law; Right of Access

## SUMÁRIO

|   |           |
|---|-----------|
| <b>INTRODUÇÃO .....</b>   | <b>12</b> |
| <b>1. DA AUTODETERMINAÇÃO INFORMATIVA À PROTEÇÃO DE DADOS PESSOAIS.....</b> | <b>16</b> |
| <b>1.1 A sociedade da informação .....</b>                                  | <b>16</b> |
| <b>1.2 A evolução do direito à privacidade.....</b>                         | <b>19</b> |
| <b>1.3 A autodeterminação informativa .....</b>                             | <b>22</b> |
| <b>1.4 As gerações de leis de dados pessoais.....</b>                       | <b>30</b> |
| <b>1.5 As iniciativas internacionais de proteção de dados .....</b>         | <b>31</b> |
| <b>1.6 Princípios da proteção de dados.....</b>                             | <b>32</b> |
| <b>2. A PROTEÇÃO DE DADOS NO BRASIL .....</b>                               | <b>35</b> |
| <b>2.1 O Habeas Data.....</b>   | <b>35</b> |
| <b>2.2 O Código de Defesa do Consumidor .....</b>                           | <b>40</b> |
| <b>2.3 A Lei do Cadastro Positivo .....</b>                                 | <b>41</b> |
| <b>2.4 A Lei de Acesso à Informação .....</b>                               | <b>44</b> |
| <b>2.5 A Lei Geral de Proteção de Dados .....</b>                           | <b>46</b> |
| <b>2.5.1 O conceito de dado pessoal .....</b>                               | <b>48</b> |
| <b>3. O DIREITO DE ACESSO AOS DADOS PELO TITULAR.....</b>                   | <b>50</b> |
| <b>3.1 Procedimento de acesso.....</b>                                      | <b>56</b> |
| <b>3.1.1 O custo do acesso .....</b>  | <b>56</b> |
| <b>3.1.2 A complexidade do acesso.....</b>                                  | <b>57</b> |
| <b>3.1.3 O formato da informação.....</b>                                   | <b>58</b> |
| <b>3.1.4 O prazo para resposta .....</b>                                    | <b>58</b> |
| <b>3.1.5 A tutela assistida para acesso aos dados.....</b>                  | <b>59</b> |
| <b>3.2 Funcionamento do acesso.....</b>                                     | <b>60</b> |
| <b>3.3 Incidência do acesso .....</b>                                       | <b>64</b> |
| <b>3.4 As dificuldades do direito de acesso e a atuação da ANPD .....</b>   | <b>65</b> |
| <b>CONCLUSÃO.....</b>   | <b>70</b> |
| <b>REFERÊNCIAS .....</b>  | <b>72</b> |

## INTRODUÇÃO

Aprovada em agosto de 2018, a Lei 13.709, conhecida como Lei Geral de Proteção de Dados (LGPD), representa um esforço político-jurídico por parte do legislador brasileiro em acompanhar a sistematização da disciplina específica acerca do tratamento de dados por diversos sistemas jurídicos através do mundo (MIRAGEM, 2019)<sup>1</sup>. Tal esforço responde a uma demanda emergente de segurança jurídica nas relações sociais fortemente baseadas nos meios eletrônicos e ligados a Internet.

Conforme trata o artigo 5º, inciso I da LGPD, considera-se dado pessoal a informação relacionada a pessoa natural identificada ou identificável. Assim, quando se é possível ligar uma informação a um indivíduo, isto é, quando um sujeito é o objeto da informação, tem-se um dado pessoal.

Nesse sentido, Danilo Doneda (2020, p. 34) ressalta que:

Uma determinada informação pode possuir um vínculo objetivo com uma pessoa revelando algo sobre ela. Esse vínculo significa que a informação refere-se às características ou ações dessa pessoa, que podem ser atribuídas a ela seja em conformidade à lei, como no caso do nome civil ou do domicílio, ou então que são informações provenientes de seus atos, como os dados referentes, por exemplo, aos seus hábitos de consumo, sobre opiniões que manifesta, à sua localização e tantas outras.<sup>2</sup>

Sendo informações relacionadas aos indivíduos, os dados pessoais estarão presentes nas mais diversas atividades que estes desenvolverem, pois quase sempre é necessário identificar-se para realizar alguma ação na sociedade.

A utilização de dados pessoais pode ocorrer por diferentes agentes privados ou públicos e para diversas finalidades. Um jornalista que desenvolve artigos de informação de interesse público pode também utilizar dados a fim de fundamentar seu trabalho, por exemplo. Entretanto, o que torna o tratamento de dados pessoais um assunto tão em voga atualmente é principalmente a utilização deles para fins econômicos.

---

<sup>1</sup> MIRAGEM, Bruno. *A Lei Geral De Proteção De Dados (Lei 13.709/2018) e o Direito Do Consumidor*. Revista dos Tribunais, v. 1009, p. 173 - 222, nov. 2019.

<sup>2</sup> DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital – Direito Privado e Internet*. 3.ed. Indaiatuba, SP: Editora Foco, 2020

Com as interações sociais e econômicas plasmadas pelo meio digital, é comum que para o desenvolvimento dos produtos e serviços disponibilizados nas redes haja a coleta de dados pessoais. Durante uma compra na internet, o fornecedor precisa do nome completo, número de CPF e endereço do consumidor para fins fiscais e da própria operação de entrega do produto escolhido. Tal prática já existia há muito no mercado, pois trata-se de uma necessidade primária de se fornecer o produto certo ao consumidor que o comprou.

Entretanto, é possível utilizar os dados também para finalidades estratégicas a fim de se especializar dentro do mercado e se tornar mais eficiente no fornecimento. Guardar o histórico de compras de um mesmo indivíduo pode ser útil na hora de oferecer um produto semelhante ao que este acabara de comprar, mas cruzar esse histórico com o de incontáveis clientes que adquiriram um mesmo item pode levar a uma indução à compra ainda mais eficaz, pois consumidores tendem ter preferências semelhantes.

Nessa lógica, é também importante para alguém que oferece um produto ou serviço na internet conhecer seu público alvo e chegar até ele através de propagandas expostas dentro do ambiente virtual que este costuma frequentar. Daí a utilização de *cookies* e outros meios informáticos a fim de conhecer o perfil do consumidor e se fazer presente nas páginas que este costuma visitar.

O surgimento dos grandes bancos de dados privados na segunda metade do último século através do desenvolvimento das tecnologias informáticas foi o que possibilitou o crescimento da capacidade de se processar dados. Antes disso, tratava-se de um processo custoso demais aos recursos privados, que não manifestavam tanto interesse dada a dificuldade de se chegar a uma informação útil a seus negócios.

A medida que as capacidades computacionais foram aumentando, o antigo monopólio dos dados pertencente aos Estados acabou sendo diluído com os agentes econômicos, que passaram a criar bancos de dados pessoais para suas finalidades privadas, intercambiando dados com outros agentes a fim de obter cada vez mais informações sobre os indivíduos.

Atualmente a economia é fortemente baseada no processamento dos dados coletados a todo instante dos indivíduos. Vários entre os maiores *players* econômicos do mundo tem suas

atividades relacionadas principalmente à tecnologia e às relações intermediadas pela internet. Há quem diga que, por estes fatores, “os dados são o novo petróleo”.

Por muito tempo, com certo vácuo legislativo no tocante a normas mais expressivas quanto ao tratamento de dados, acompanhando o desenvolvimento mundial, a prática do tratamento de dados no Brasil se desenvolveu exponencialmente através das tecnologias como do processamento informático. Com a coleta massiva de dados pessoais em diversos meios, principalmente eletrônicos, e o processamento destes, é possível inferir um perfil do usuário com diversas informações sobre ele. Tal perfil pode conter informações sobre o que o indivíduo gosta ou não de fazer, assuntos que o interessam e inclusive convicções políticas e religiosas, que correspondem a uma esfera ainda mais íntima de sua privacidade.

Estes perfis, entretanto, eram praticamente inalcançáveis pelos titulares<sup>3</sup> dos dados, que muito pouco sabiam do que era conhecido sobre si mesmo no mercado. Tal perspectiva tende a se modificar com a adequação dos atores econômicos à nova lei.

A proteção dos dados pessoais visa, entre outras coisas, garantir o controle do titular sobre quais dados seus podem ser tratados e o que se pode fazer com eles. Entretanto, para que haja uma efetivação desse controle pelo titular é necessário que este tenha facilidade de acesso aos dados coletados pelos agentes de tratamento. Como ressalta a própria LGPD, um dos princípios a serem observados quando realizadas as atividades de tratamento de dados pessoais é o livre acesso, que é descrito como a “*garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais*”<sup>4</sup>.

Prescrito não só como princípio, mas também como direito material, o direito de acesso aos dados decorre também do fundamento da autodeterminação informativa, trazendo uma nova perspectiva para a atividade de tratamento de dados à medida que torna o titular um participante do processo que transforma seus dados em informações a seu respeito. A partir disso, cria-se a necessidade de maior transparência nas relações entre o titular dos dados e os agentes econômicos que se interessam por esses bens, fortalecendo a parte mais vulnerável que

---

<sup>3</sup> Titular é o termo definido pela LGPD em seu art. 5º, V, como pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

<sup>4</sup> LGPD, Art 6º, IV.

passa a ter a possibilidade de visualizar-se dentro do processo de tratamento que utiliza seus dados.

O presente estudo se propõe a entender o contexto e o desenvolvimento do direito à proteção de dados pessoais no mundo a partir das necessidades de se tutelar a personalidade humana ao longo dos anos. Além disso, dada a necessidade de se estudar a efetivação desse direito no Brasil, tendo em vista o atual estágio do desenvolvimento tecnológico e a cultura de tratamento praticada antes da lei, a pesquisa também visa estudar o panorama protetivo no tocante ao processamento de dados no ordenamento jurídico brasileiro antes da chegada da LGPD. Por fim, busca-se entender a real importância do direito de acesso na proteção de dados, o que ele abrange, como deve ser garantido, como foi concebido na LGPD, quais as consequências práticas de se garantir tal direito ao titular e o que pode contribuir para a garantia desse direito aos titulares de dados pessoais.

## 1. DA AUTODETERMINAÇÃO INFORMATIVA À PROTEÇÃO DE DADOS PESSOAIS

### 1.1 A sociedade da informação

Ao longo da história, a estruturação da sociedade teve diversos protagonistas que balizavam as transformações entre as formas de se produzir. O início da exploração da terra pelo homem há milhares de anos configurou a chamada sociedade agrícola através do desenvolvimento das técnicas de plantio, possibilitando o cultivo não somente para consumo próprio, mas a especialização e troca entre diferentes produtores especializados em cultivar determinados gêneros alimentícios vegetais em escala que ultrapassava a necessidade doméstica.

Tempos depois, a produção manufaturada artesanal deu lugar às máquinas de vapor que ampliaram indefinidamente as capacidades produtivas através das fábricas. Era possível, num curto espaço de tempo, produzir muito mais do que se o mesmo número de funcionários trabalhasse individualmente como artesãos. Os maquinários movidos a combustíveis levaram à chamada sociedade industrial, em que a forma de produzir foi completamente alterada, trazendo mudanças no mundo do trabalho e na circulação econômica. Dentro ainda da sociedade industrial, a modernização advinda da eletricidade trouxe, com a segunda revolução Industrial, o fortalecimento deste modelo produtivo baseado nas fábricas.

Após a era pós-industrial, caracterizada pela centralidade do fornecimento de serviços, a informação é hoje o foco e base das relações sociais da chamada Sociedade da Informação (BIONI, 2020)<sup>5</sup>. Nesta nova configuração, não se tem mais como centro a produção de bens físicos, mas o desenvolvimento da produção “*por meio do acúmulo de conhecimento e da facilitação de seu acesso pelas pessoas*”, garantindo, assim, o “*acesso aos bens tangíveis e corpóreos através dos bens intangíveis e incorpóreos*” (LISBOA, 2006)<sup>6</sup>.

---

<sup>5</sup> BIONI, Bruno. *Proteção de Dados Pessoais – A Função e os Limites do Consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 5.

<sup>6</sup> LISBOA, Roberto Senise. Direito na sociedade da informação. *Revista dos Tribunais*, ano 95, v. 847, p. 78-95, mai. 2006. p. 8.



É equivocado, entretanto, dizer que esta forma de organização social corresponda somente ao ambiente virtual, ainda que seja clara a contribuição da informática e da Internet para a formação da sociedade hoje vivenciada.

Para que uma pessoa possa se mover numa sociedade baseada na informação, frequentemente ela precisa fornecer dados para ser identificada, para autorizar uma transação e inclusive para ser representada em situações onde sua presença física não é possível (DONEDA, 2020)<sup>7</sup>. As tecnologias informacionais facilitaram a coleta, o armazenamento e a utilização ampla de informações pessoais para as mais diversas finalidades, o que possibilitou o crescimento das atividades voltadas para esse fim.

Conforme assinala Márcio Laeber (2007, p. 2):

O desenvolvimento tecnológico permitiu a substituição das antigas fichas cadastrais manuais por arquivos eletrônicos que, dispostos em poderosos computadores e tratados por poderosos programas, são capazes de cruzar informações pessoais com precisão e eficiência jamais vistas.

A evolução acelerada da informática e da telemática derrubaram fronteiras geográficas no transporte da informação, mormente com o surgimento da internet, permitindo, em curto espaço de tempo, relacionar dados contidos em diferentes bancos de dados em diferentes locais do mundo.<sup>8</sup>

Hoje, o cruzamento dos dados não é mais feito manualmente como outrora. Enquanto antigamente era necessário que cada ficha de informação fosse analisada individualmente por um agente que tomaria uma decisão, hoje temos máquinas capazes de computar estes dados em velocidades e volume extremamente maior.

Com a criação do computador, houve o aperfeiçoamento dos sistemas de bens de produção e comunicação de forma que as relações foram amplamente afetadas, conforme destaca Lisboa (2006, p. 15):

A informática transformou o mundo, porém a sua revolução não suprimiu o que se havia feito no passado: os sistemas de produção de bens não se encontram apenas mecanizados, como também eletrônicos, e por programas de dados; a grande maioria dos negócios jurídicos são realizados mediante o processo de computação, ainda que não celebrados pela via virtual; os sistemas de transporte submetem-se a

<sup>7</sup> DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital – Direito Privado e Internet*. 3.ed. Indaiatuba, SP: Editora Foco, 2020

<sup>8</sup> LAEBER, Márcio Rafael Silva. Proteção de Dados Pessoais: O Direito à Autodeterminação Informativa. *Revista de Direito Bancário e do Mercado de Capitais*, v. 37, p. 59-80, jul-set 2007

programas de dados para o funcionamento dos coletivos (como sucede, por exemplo, com o metrô); a biotecnologia se utiliza de processos novos para o diagnóstico e o tratamento de doenças; o controle dos poluentes passa a ter um eficaz aliado a partir da utilização do programa de dados. Ou seja: a Sociedade da Informação veio aprimorar o convívio social, colaborando para o progresso e facilitando o acesso à informação, inclusive para os fins de celebração do ato e do negócio jurídico.<sup>9</sup>

Conforme o autor relata, com o crescimento da influência dos meios informacionais na sociedade tem-se um movimento socioeconômico de transnacionalização, já que grandes empresas passam a ter maior poder de operação num mundo mais conectado. O e-commerce cresce até ter protagonismo em determinados setores em detrimento do comércio físico. Além disso, a informação passa a ter um valor econômico, pois passa a ser um ativo intelectual (um patrimônio da pessoa). Tem-se também uma ampla formação de bancos de dados e o aumento da transferência eletrônica desses dados.

Para Lisboa (2006, p. 11), a economia da informação, também chamada de economia do conhecimento, é baseada em 3 fundamentos: a) *o conhecimento impregna tudo o que compramos, vendemos e produzimos*; b) os ativos financeiros e físicos tem menos importância para as empresas que o capital intelectual; c) as novas técnicas de gestão e estratégia, bem como as novas tecnologias são a forma de beneficiar-se desses ativos e crescer na economia.<sup>10</sup>

O processamento dos bancos de dados por meios informatizados, quando comparado ao processamento manual, é capaz, a partir da possibilidade de um grande armazenamento de dados pessoais, combinar tais dados de forma antes impossível, gerando resultados de forma muito mais rápida e eficiente que a prática anterior. Nesse sentido, entende Danilo Doneda (2019, p. 141) que é um “*elemento catalisador de um novo perfil de utilização de informação*” que se apresenta com tal importância que a maioria das normas sobre proteção de dados que seriam produzidas tratariam de sua regulação de forma tangenciada ou até exclusiva<sup>11</sup>.

A preocupação com a regulação das atividades que armazenavam e processavam dados pessoais através dos avanços da capacidade computacional, visava inicialmente criar normas e procedimentos para a utilização das informações pessoais pelos bancos de dados, que estavam em amplo desenvolvimento. As iniciativas eram muitas vezes direcionadas à regulação em

<sup>9</sup> LISBOA, Roberto Senise. Direito na sociedade da informação. *Revista dos Tribunais*, ano 95, v. 847, p. 78-95, mai 2006. p. 15.

<sup>10</sup> Ibidem, p11.

<sup>11</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019

contextos específicos, como as normas atinentes à proteção das informações de movimentações bancárias, como o sigilo bancário, por exemplo.

O referido autor denuncia, entretanto, a deficiência que tais modelos apresentam na proteção dos indivíduos, por estarem demasiadamente restritos à certos contextos:

Esta setorização, em si, pode ter diversas consequências, entre elas o próprio enfraquecimento da tutela da pessoa, por esta ficar dependente de contextos setoriais, e não da noção da proteção do indivíduo em si (caso típico, justamente, do sigilo bancário). Em outra dimensão, a setorização pode ser útil para a especificação da abordagem a ser dada a partir das especificidades de cada setor.<sup>12</sup>

Como se pretende apresentar neste estudo, a normatização da proteção de dados pessoais não deve se restringir à regulação puramente das atividades de processamento eletrônicas, mas também de toda atividade que envolva a coleta, armazenamento, cruzamento de informações e inclusive transmissão destas a outros interessados de modo a proteger os indivíduos de usos abusivos de seus dados. Além disso, à disciplina de proteção de dados deve ter em sua essência a tutela dos direitos relacionados à pessoa humana, sem deixar de considerar o contexto social que depende do processamento de dados para o desenvolvimento econômico e comunitário.

## 1.2 A evolução do direito à privacidade

A privacidade por muito tempo foi entendida como a preservação de um isolamento, de um refúgio ou segredo. Ela começou a ser estudada nos ordenamentos jurídicos principalmente no final do século XIX, como se pode depreender do estudo realizado por Brandeis e Warren, *The right to privacy*.

Ela era associada, inicialmente ao direito de ser deixado só, o direito do indivíduo de não sofrer a interferência do Estado sobre certa parcela de sua vida. Além disso, também, se trata de um direito ligado à proteção do indivíduo, por parte do Estado, das interferências de terceiros em sua vida.

---

<sup>12</sup> Ibidem, p. 141-142.

O Sigilo ou segredo, com os quais há uma identificação com a privacidade, correspondem à proibição de se tomar conhecimento e de divulgar determinadas informações que se encontram numa esfera protegida da vida do indivíduo.

Cabe ressaltar ainda que há para certos ramos da doutrina a separação entre direito à intimidade e direito à privacidade, conforme assinala Alessandro Hirata (2017):

A. De Cupis, por exemplo, entende que a esfera íntima da pessoa se divide em direito à *riservatezza* e o direito à *segretezza*. O direito à intimidade pode ser conceituado como aquele que visa a resguardar as pessoas dos sentidos alheios, principalmente da vista e dos ouvidos de outrem. Ou seja, é o direito da pessoa de excluir do conhecimento de terceiros tudo aquilo que a ela se relaciona. O direito à intimidade é, ainda, o poder correspondente ao dever de todas as outras pessoas de não se imiscuir na intimidade alheia, opondo-se a eventuais descumprimentos desse dever, realizados por meio de investigação e/ou divulgação de informações sobre a vida alheia.<sup>13</sup>

Entretanto, conforme a sociedade foi se desenvolvendo, os debates sobre a privacidade tiveram que acompanhar tal evolução a fim de garantirem direitos ideais à realidade temporal a que os indivíduos vivenciavam.

Bernard Edelman (1999, p. 53) apresenta interessante reflexão acerca da necessidade de se acompanhar a evolução tecnológica:

“Se por um lado o direito não julga a ciência, por outro ele não tem dúvidas de que ela existe e de que produz efeitos na ordem jurídica: A biologia revolucionou a visão jurídica do homem e da natureza, a informática, aquela dos direitos de autor e dos direitos da personalidade, a pesquisa nuclear renovou a ideia de soberania e de responsabilidade. Dito de outra forma a evolução das ciências e das técnicas não é indiferente ao direito.”<sup>14</sup>

Considerando que o Direito é pensado e planejado para ser um instrumento de pacificação social, protegendo a pessoa humana de ataques injustos à sua existência, desconsiderar os avanços tecnológicos é apartar o Direito da realidade, “*tornando-o anacrônico, incapaz de*

<sup>13</sup> HIRATA, Alessandro. Direito à privacidade. *Enciclopédia jurídica da PUC-SP*. CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (Coord.). Tomo: Direito Administrativo e Constitucional. NUNES JUNIOR, Vidal Serrano; ZOCKUN, Maurício; ZOCKUN, Carolina Zancaner, FREIRE, André Luiz (Coord. de Tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> - Acesso em 29 de outubro de 2020.

<sup>14</sup> EDELMAN, Bernard. *La personne en danger*. Paris: Puf, 1999. p. 377. apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 53.

*enquadrar os interesses da pessoa com a velocidade característica da tecnologia.*”(DONEDA, 2020).<sup>15</sup>

Os debates acerca dos direitos da personalidade, foram cruciais para a evolução do conceito de privacidade meramente individualista para uma proteção que garanta o livre desenvolvimento da personalidade humana.

Esta preocupação em se proteger mais efetivamente os interesses existenciais da pessoa humana data desde a Constituição de Weimar, no início do século XX, mas toma força num movimento global após os eventos ocorridos na II Guerra Mundial, principalmente com influência da Declaração Universal de Direitos Humanos da Organização das Nações Unidas, que inicia seu preâmbulo afirmando que: *“o reconhecimento da dignidade inerente a todos os membros da família humana e dos seus direitos iguais e inalienáveis constitui o fundamento da liberdade, da justiça e da paz no mundo”*.

O princípio da dignidade humana passa a mudar o foco das legislações, que antes tinham uma preocupação muito maior com o âmbito patrimonial, para a tutela do ser humano e sua existência (BIONI, 2020). Ele nasce para tutelar a existência do ser humano, o respeito a existência individual da pessoa considerando que todas as pessoas merecem tal reconhecimento.

Para Kant (2000, p. 68), o homem *“existe como um fim em si mesmo, não só como meio para o uso arbitrário desta ou daquela vontade. Pelo contrário, em todas as suas ações, tanto nas que se dirigem a ele mesmo, como nas que dirigem aos outros seres racionais, ele tem de ser considerado simultaneamente como fim”*<sup>16</sup>. Assim, o ser humano não pode ser considerado um meio, um instrumento, um objeto de valor, mas um ser que deve ser dotado de dignidade e reconhecido como sujeito. Deve ser livre para se desenvolver e estabelecer relações com os demais indivíduos. Conforme o homem é capaz de agir no mundo e ser reconhecido como sujeito único, ele é capaz de construir uma identidade.<sup>17</sup>

<sup>15</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 54.

<sup>16</sup> KANT, Immanuel. *Fundamentos da metafísica do costume*. Tradução: Paulo Quintela. Lisboa: Edições 70, 2000. p. 68.

<sup>17</sup> Conforme cita Hasso Hofmann: “o homem ganha sua própria dignidade enquanto autodetermina seu próprio comportamento e, assim, constrói para si uma identidade”. HOFMANN, Hasso. *La promessa della dignità*

Além da dignidade humana, o livre desenvolvimento da personalidade é direito importante na evolução da proteção humana e de sua autonomia. Sobre esse direito, fala Felipe Arady Miranda (2013, p. 11207):

O direito ao livre desenvolvimento da personalidade protege um direito de liberdade individual em relação à constituição da personalidade, sendo um direito do indivíduo desenvolver sua personalidade de forma livre, sem a intervenção de terceiros, agindo, ou deixando de agir de acordo com a sua convicção. Portanto, esse direito emana um conteúdo positivo, na liberdade de agir, e um conteúdo negativo, na não interferência ou impedimentos. Nessa perspectiva, chegou-se ao entendimento de que tal direito corresponde a duas facetas, o direito geral de personalidade (proteção abrangente de todas as formas de lesão de bens de personalidade independentemente de estarem ou não tipicamente consagrados) e a liberdade geral de ação (liberdade do indivíduo agir, ou deixar de agir, de acordo com suas convicções). Quanto ao conceito de liberdade inerente ao desenvolvimento da personalidade, entendemos que não há como diferenciar o que constitui o núcleo da personalidade do indivíduo, e o que é apenas um direito reflexo de personalidade e que não corresponde diretamente ao seu desenvolvimento. Portanto, todas as manifestações da personalidade estão abarcadas pelo sistema de proteção, mesmo que esta não esteja diretamente relacionada ao seu desenvolvimento.<sup>18</sup>

### 1.3 A autodeterminação informativa

Com o desenvolvimento de projetos de construção de grandes estruturas computacionais para o processamento de dados pessoais na década de 1960, juristas americanos e europeus começaram a debater sobre a possibilidade de danos decorrentes de tais processamentos (LAEBER, 2007)<sup>19</sup>.

É nesse momento que surgem nos Estados Unidos os primeiros instrumentos voltados a regular as atividades dos bancos de dados de proteção ao crédito, como o *Fair Credit Reporting Act* (FCRA), de 1970. Poucos anos depois, é aprovada em solo americano uma lei direcionada a proteção da privacidade dos cidadãos, o *Privacy Act*, em 1974.

---

*umana*. Rivista Internazionale di Filosofia del Diritto, IV serie. v. 76, p. 620-650, 1999, apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 76.

<sup>18</sup> MIRANDA, Felipe Arady. O Direito Fundamental ao Livre Desenvolvimento da Personalidade. *Revista do Instituto do Direito Brasileiro*, Ano 2, n. 10, p. 11175-11211, Lisboa, 2013.

<sup>19</sup> LAEBER, Márcio Rafael Silva. Proteção de Dados Pessoais: O Direito à Autodeterminação Informativa. *Revista de Direito Bancário e do Mercado de Capitais*, v. 37, p. 59-80, jul-set 2007.

No velho continente, eram aprovadas a essa época, as primeiras leis relacionadas à disciplina do processamento de dados pelos bancos de dados eletrônicos. Pode-se citar a primeira lei de proteção de dados do *Land*<sup>20</sup> alemão de Hesse, em 1970, e a *Datalog*, na Suécia, em 1973. Em 1977, a República Federal da Alemanha aprovou também, uma lei federal de proteção de dados, a *Bundesdatenschutzgesetz*.

As normativas eram pensadas num contexto de mudança informacional no mundo desenvolvido visando grandes centros de processamento de dados. Eram voltadas à permissão estatal para o funcionamento e controle dos bancos de dados por parte dos governos.

Uma das primeiras preocupações do legislador brasileiro ao conceber a LGPD foi definir os fundamentos da proteção de dados em seu artigo 2º:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

**II - a autodeterminação informativa;**

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A autodeterminação informativa, elencada entre os fundamentos ou princípios da proteção de dados proposta pela nova lei é um conceito que remete inicialmente ao ano de 1983, na Alemanha Ocidental, onde foi proclamada como direito fundamental pelo Tribunal Constitucional em julgamento acerca da “Lei do Recenseamento de População, Profissão, Moradia e Trabalho”.

A referida lei propunha a coleta de dados pessoais de cidadãos através de um questionário de 160 perguntas, cujas informações seriam processadas de maneira informatizada, sendo punidos com multas elevadas aqueles que não o respondessem. A questão gerou sentimento de insegurança quanto a maneira com que seriam tratados os dados e quanto às finalidades das informações geradas pelo tratamento, o que levou ao julgamento da inconstitucionalidade

<sup>20</sup>

*Land* equivale a um estado ou província.

parcial do diploma pelo reconhecimento da corte do direito do indivíduo de ter o livre controle sobre o fluxo de suas informações na sociedade.<sup>21</sup>

O Tribunal entendeu que a interpretação da proteção dos direitos fundamentais deveria ser desenvolvida sempre considerando as mudanças sociais e tecnológicas que se apresentavam de modo a superar as novas ameaças que surgiam (MENDES, 2018)<sup>22</sup>.

No caso da lei do Recenseamento, entendeu o tribunal que com o processamento dos dados seria possível elaborar um “quadro completo da personalidade” através de “sistemas integrados sem que o interessado possa controlar o suficiente sua correção e aplicação”. Tal realidade limitaria a liberdade de decisão do indivíduo, que se veria preso “da pressão psíquica da participação pública” e conseqüentemente, sob forte influência do poder estatal.

Como assinala Laura Schertel Mendes (2018, p. 189), concebeu o tribunal alemão um direito à autodeterminação informativa que se entendia como “*o poder do indivíduo em determinar fundamentalmente por si mesmo sobre a coleta e utilização de seus dados pessoais*”, derivado da privacidade, mas que à extrapolava, já que com o aumento da capacidade de processamento eletrônico, não se podia mais entender a existência de dados insignificantes<sup>23</sup>. A ameaça de lesão aos direitos da personalidade dos indivíduos pelo processamento dos dados estava mais pautada nos objetivos do processamento e de que forma ele acontecia do que nos dados em si e se eram íntimos ou não.

A autora cita a insuficiência da privacidade puramente considerada como fundamento da proteção de dados na lei de recenseamento:

Duas foram as principais críticas da doutrina alemã à fórmula da esfera privada que acabaram por motivar a evolução desse conceito. A primeira crítica refere-se à relatividade da esfera privada, isto é, ao fato de que os desejos de privacidade podem diferir muito fortemente de pessoa para pessoa. Assim, espaços não poderiam ser designados rigidamente de esfera privada ou íntima, “pois os espaços vitais, nos quais o indivíduo se refugia para descansar das exigências sociais, preparar um comportamento social e fazer tudo o que não pode ser trazido para a sociedade e representado diante dela são relativos”. A segunda crítica, estreitamente relacionada

<sup>21</sup> BVerfGE 65, 1, *Volkszählung* (Recenseamento), 1983. apud MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

<sup>22</sup> MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

<sup>23</sup> Ibidem.



ao princípio da relatividade da esfera privada, refere-se ao contexto de aplicação. Ela se refere à ideia básica de que “a sensibilidade e o significado das informações dependem do respectivo contexto de aplicação” e não podem ser definidos *a priori* somente pelo conteúdo da informação, isto é, se é íntimo, privado ou público. Assim, a finalidade do levantamento e o destinatário da informação são muito mais decisivos para a avaliação da constitucionalidade do processamento de dados do que a classificação de dados em esfera privada e íntima.<sup>24</sup>

Danilo Doneda (2020, p. 166), por sua vez, reflete que o sentimento de insegurança na sociedade alemã na época da edição da lei do censo se dava pelas possibilidades de usos dos dados obtidos pelo governo. O texto legal permitiria que os dados obtidos fossem “*confrontados com os dados do registro civil para uma eventual retificação do próprio registro*”, e que “*desde que não identificados com o nome de cada titular, pudessem ser transmitidos às autoridades federais aos Lander*”. Além disso, havia a previsão da cobrança de uma alta multa pecuniária para os cidadãos que não participassem do censo, assim como formas de favorecer quem os denunciasse. Tais aspectos da lei evidenciavam um aparente intento do poder público em controlar os cidadãos, à medida que possibilitaria, além do atendimento das finalidades estatísticas, saber com demasiado detalhe as condições dos cidadãos.

Dada a vigência da lei federal de proteção de dados alemã desde 1977, era de se esperar que tais problemas fossem sanados com a aplicação da mesma. Entretanto, não foi possível garantir-se tal proteção em face da lei do censo, pois, anos antes, já havia decisão administrativa de que “*as leis relativas à coleta de dados para fins estatísticos prevaleceriam, em caso de conflito, sobre a lei federal de proteção de dados pessoais*”<sup>25</sup>

A Corte constitucional alemã foi convencida de que o censo aprovado iria de encontro aos direitos da personalidade. Um dos motivos foi que se percebeu que utilizar os dados pessoais dos cidadãos para fins administrativos e estatísticos demonstrava a diversidade de finalidades, fazendo com que não houvesse clareza ao cidadão do objetivo do processamento de seus dados. Como o rigor estatístico, voltado a demonstrar resultados de acordo com conjuntos de indivíduos e discrepâncias de informações, não se alinha com a necessidade de identificação dos titulares dos dados pelo poder público, ficava caracterizada incompatibilidade entre as finalidades. Com isso, chegou-se ao entendimento de que as atividades de

---

<sup>24</sup> Ibidem. p. 189.

<sup>25</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 166.

processamentos de dados pessoais deveriam ser norteadas por uma finalidade específica, demonstrada na coleta de tais dados (DONEDA, 2020).<sup>26</sup>

Nos termos da sentença:

não se pode levar em consideração somente a natureza das informações; são determinantes, porém, a sua necessidade e utilização. Estas dependem em parte da finalidade para a qual a coleta de dados é destinada, e de outra parte, da possibilidade de elaboração e de conexão próprias da tecnologia da informação. Nesta situação, um dado que, em si, não aparenta possuir nenhuma importância, pode adquirir um novo valor; portanto, nas atuais condições do processamento automático de dados, não existe mais um dado ‘sem importância’<sup>27</sup>

Como ressalta Mendes (2018, p. 191), o julgamento pauta-se principalmente em três questões:

Primeiramente, o poder de decisão é formulado como o teor da proteção de modo que o indivíduo pode decidir, ele próprio, sobre a coleta e a utilização de informações de cunho pessoal. Daí resulta a segunda propriedade, ou seja, a de que o direito fundamental à autodeterminação informativa não abrange um teor de proteção fixo e definido, desviando-se, assim, do modelo de esfera privada de atribuição de dados a uma esfera íntima. Em terceiro lugar, a referência à pessoa atua decisivamente sobre o teor da proteção na medida em que cada registro que se revela como pessoal é merecedor de proteção.<sup>28</sup>

São, então, 3 as características principais da constituição do direito à autodeterminação informativa: ele é um direito protetivo que garante ao indivíduo o poder de decidir sobre quando e como seus dados podem ser utilizados; essa proteção extrapola a dimensão da privacidade isoladamente considerada, protegendo de forma mais flexível o indivíduo; e a tutela de qualquer dado que se relacione à pessoa, garantindo-lhe proteção.

A autora ensina que a decisão da corte alemã em 1983 além de ter evoluído um debate jurídico necessário para a fundamentação do direito à autodeterminação informativa, também contribuiu para a consolidação do direito geral da personalidade “*como um projeto efetivo, flexível e de aplicação prática*” (MENDES, 2018).

<sup>26</sup> Ibidem. p. 167.

<sup>27</sup> FROSINI, Vittorio. *Contributi ad un diritto dell'informazione*. Napoli: Liguori, 1991. cit., pp. 128-129 apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

<sup>28</sup> MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018. p. 191.

O direito à autodeterminação informativa não se trata de um direito rígido e fixo, mas de uma proteção abstrata muito mais relacionada ao poder de decisão. Não é a proibição do uso dos dados, mas a garantia de que o indivíduo participe do processo de tomada de decisão que envolve a utilização dos seus dados. Assim, quando houvesse atividades de coleta, processamento ou transmissão de dados pessoais, a autodeterminação informativa se aplicaria graças a flexibilidade de aplicação de tal direito.

No desenvolvimento do direito à proteção de dados, distanciou-se da proteção fixa, outrora relacionada somente à esfera íntima ou privada, para o empoderamento do indivíduo através da possibilidade de decidir sobre seus dados e para a regulação de quais limites devem ser observados nas atividades de processamentos de informações pessoais.<sup>29</sup>

Nesse sentido, Catarina Sarmiento e Castro (2002, p. 476-477) destaca que:

[O direito à autodeterminação informativa] traduz-se num feixe de prerrogativas que pretendem garantir que cada um de nós não caminhe nu, desprovido de um manto de penumbra, numa sociedade que sabe cada vez mais acerca de cada indivíduo. É um direito a não viver num mundo com paredes de vidro, é um direito a não ser transparente, por isso, desenha-se como um direito de proteção, de sentido negativo. Visto deste prisma, o direito em causa permite que o indivíduo negue informação pessoal, se oponha à sua recolha, difusão, ou qualquer outro modo de tratamento. Neste sentido, ainda está próximo da ideia Americana de '*privacy*', enquanto direito de defesa face às agressões do Estado e terceiros às suas informações pessoais. Mas é mais. Longe de ser um mero direito contra as intrusões do Estado ou de outros indivíduos, que devem abster-se de proceder a tratamentos dos seus dados pessoais, é um direito a decidir até onde vai a sombra que deseja que paire sobre as informações que lhe respeitam, construindo-se como uma liberdade, como um poder de determinar o uso dos seus dados pessoais. Assim, evita-se que o indivíduo se transforme em 'simples objeto de informações' também na medida em que se lhe atribui um poder positivo de dispor sobre as suas informações pessoais, i.e., um poder de autotutela, de controle, sobre os seus dados pessoais, que permite ao cidadão 'preservar a sua própria identidade informática'.<sup>30</sup>

---

<sup>29</sup> Ibidem.

<sup>30</sup> CASTRO, Catarina Sarmiento. Os ficheiros de crédito e a protecção de dados pessoais. *Boletim da Faculdade de Direito*, Coimbra, v. LXXVII, 2002, p. 476-477. apud LAEBER, Márcio Rafael Silva. Proteção de Dados Pessoais: O Direito à Autodeterminação Informativa. *Revista de Direito Bancário e do Mercado de Capitais*, v. 37, p. 59-80, jul-set 2007.

Com toda a questão da inconstitucionalidade da lei em 1983, foi necessária a edição de uma nova lei, anos seguintes, corrigindo os pontos debatidos. Foi então, que em 1985 a Alemanha promulgou uma nova lei para disciplinar o recenseamento que ocorreria em 1987, desta vez, observando os limites da autodeterminação informativa dos cidadãos.

Conforme foi entendido na época e com o desenvolvimento mais abrangente na União Europeia nos anos que se seguiram, o direito à autodeterminação informativa figurava como um direito material que permitia ao indivíduo decidir que partes de sua intimidade seria revelada, opondo-se ao total controle de sua vida pelo Estado. Com a efetivação desse direito protegem-se a dignidade humana e a livre formação da personalidade.

Há, entretanto, posições contrárias quanto ao termo que fundamentou a decisão em 1983 e muitas leis de proteção de dados que se seguiram, como destaca Danilo Doneda (2019, p. 170):

deparamo-nos com o problema da interpretação sobre o que é a "autodeterminação". Em uma hipótese, ela conferiria ao indivíduo a oportunidade de controlar as informações que lhe digam respeito. dentro de parâmetros de ampla informação e solidariedade, já em uma leitura em chave liberal, a autodeterminação estaria concentrada no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais, e assim poderia se prestar ao afastamento da matéria do âmbito dos direitos da personalidade. Outro problema é que esta leitura pode induzir a impressão de que as pessoas teriam um direito de propriedade sobre suas informações, transportando esta fenomenologia para o campo das situações patrimoniais. Tais problemas, por mais que sejam objetáveis, acabaram por constituir um embargo para uma disseminação mais ampla do direito à auto determinação informativa<sup>31</sup>

Assim, ainda que o conceito definido na Alemanha tenha sido base para toda uma construção da proteção de dados em vários países posteriormente, houve países que se opuseram a tal termo, por entender não ser suficiente à proteção da capacidade dos indivíduos de desenvolver livremente sua personalidade através do controle de seus dados.

Um desses países foi o Chile, que no processo legislativo que debatia o projeto de lei de proteção de dados pessoais no país, excluiu o termo “autodeterminação informativa” fundamentando que sua utilização levaria a um risco de “patrimonialização”.<sup>32</sup>

---

<sup>31</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

<sup>32</sup> Como cita Danilo Doneda em sua obra DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019., referindo-se a texto de Francisco González Hock.

Alguns destes países, principalmente a Espanha e alguns da América hispânica, preferiram utilizar o termo liberdade informática, definido por Pérez Luño (1989, apud DONEDA, 2019, p. 170) como:

garantir a faculdade das pessoas de conhecer e acessar as informações que lhes digam respeito, arquivadas em bancos de dados, controlar sua qualidade, o que implica a possibilidade de corrigir ou apagar os dados inexatos ou indevidamente processados; e dispor sobre a sua transmissão<sup>33</sup>

Doneda (2019, p. 171) entende, porém, que há problemas na utilização do termo liberdade informática:

A noção de uma "liberdade informática" como resposta às questões trazidas pelo processamento de dados pessoais merece, porém, ressalvas: ao fazer referência direta à liberdade, utiliza-se de um conceito bastante amplo que, em determinados contextos, carece de uma ligação mais estreita com a trajetória histórica dos direitos fundamentais e seus mais recentes avanços (entre os quais a própria tutela dos dados pessoais); assim tornando também possível uma interpretação "hipertrofiada" da possibilidade de autodeterminação, que abstrai o conjunto de problemas relativos à informação, aos quais nos aludimos quando tratamos da autodeterminação informativa. O outro problema diz respeito à referência à informática: muito embora a mencionada "consciência tecnológica" de Frosini seja indispensável a todo jurista, a estruturação de categorias gerais em torno de fenômenos tecnológicos como a informática pode contribuir à redução de seus efeitos e também à sua rápida obsolescência. Particularmente em relação à informática, a crítica que podemos fazer (valendo-nos das décadas que nos separam) é a de que os efeitos das tecnologias informáticas penetraram de tal modo em várias instâncias da vida dos cidadãos, sejam usuários diretos ou não de computadores, que separar os fenômenos relativos à informática de outros ("tradicionais", digamos) tornou-se ao mesmo tempo impossível e irrelevante. Deve-se, por outro lado, reforçar as categorias tradicionais com vistas aos fenômenos advindos com a tecnologia e com a informática, pois separá-los seria, hoje, contraproducente. A tal ponto a informática está presente no nosso cotidiano que individuar os casos nos quais ela é aplicada é tarefa destinada ao mais retumbante fracasso.<sup>34</sup>

Defende, então, a utilização de um termo mais simples, que abrange tanto a questão da privacidade, quanto a da informação, sem permanecer num campo muito conceitual, nem correr o risco de uma interpretação patrimonialista: a proteção de dados pessoais.

<sup>33</sup> PÉREZ LUÑO, Antonio-Enrique. Los derechos humanos en la sociedad tecnológica, in: LOSANO, Mario; PÉREZ LUÑO, Antonio-Enrique; GUERRERO MATEUS, Maria Fernanda. *Libertad informática y leyes de protección de datos personales*. Madrid: Centro de Estudios Constitucionales, 1989, p. 155. apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 170-171.

<sup>34</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

## 1.4 As gerações de leis de dados pessoais

A primeira geração de leis de dados pessoais era caracterizada pela concessão de autorizações para a criação de bancos de dados e do seu controle posterior pelo poder público, entretanto eram muito voltadas para as técnicas de processamento, sem garantir uma efetiva participação dos cidadãos. Exemplos dessas leis são a lei do *Land* de Hesse na Alemanha, em 1970; o *Data Legen 289* ou *Datalog*<sup>35</sup>, um estatuto para bancos de dados na Suécia, em 1973; e o *Privacy Act* dos Estados Unidos em 1974.

Na segunda geração de leis, já era possível observar uma evolução na preocupação com o processamento dos dados por meios informáticos, já que levava em conta a privacidade e considerava a proteção dos dados pessoais como uma liberdade negativa. Entre as aprovadas nessa época pode-se citar a lei francesa de Proteção de dados (*Informatique et Libertés*<sup>36</sup>) e a lei austríaca (*Datenschutzgesetz*)<sup>37</sup>, ambas de 1978.

A decisão da Corte Alemã marca a terceira geração de leis de dados na década de 1980. A partir de tal decisão que houve emendas às leis já existentes na própria Alemanha e na Áustria, bem como novas leis específicas na Noruega e na Finlândia. A tutela dos dados pessoais buscava neste momento garantir efetividade da liberdade de fornecer ou não os dados, preocupando-se também com o contexto do fornecimento de dados pelos cidadãos a fim de protegê-lo quanto abusos que o impedissem de manifestar sua escolha, dando maior voz e participação aos indivíduos quanto ao processamento de seus dados, através do reconhecimento da autodeterminação informativa, e prevendo que os interessados deviam informar melhor os titulares, também em vias de participá-lo como ser ativo na utilização de suas informações.

As leis mais recentes, inclusive a LGPD, encaixam-se na chamada quarta geração de leis. São atentas a questão de que não só o indivíduo titular isoladamente considerado é vulnerável ante aos interessados no tratamento de dados, mas toda a coletividade que com tais organizações se relacionam. Propõem, então, medidas como as multas por descumprimento para tutelar o direito à proteção de dados. Além disso, reconhecem a existência de dados que necessitam de maior proteção e, por isso, seu tratamento precisa ser condicionado não apenas por decisões

---

<sup>35</sup> *Datalog* 1973:289, de 11 de maio de 1973.

<sup>36</sup> Lei 78-17, de 6 de janeiro de 1978.

<sup>37</sup> Lei de 18 de outubro de 1978, n° 565/1978.

individuais dos indivíduos. O estímulo à criação de autoridades independentes para a tutela dos direitos garantidos nessas leis também é um ponto bem comum nas leis da quarta geração.

### 1.5 As iniciativas internacionais de proteção de dados

Como o processo do desenvolvimento econômico passa pela transnacionalização do mercado, pode-se chegar à conclusão de que os dados pessoais estariam envolvidos nesse movimento de globalização. Assim, houveram ao longo do tempo esforços coletivos de se regular a circulação de dados entre os países.

No fim da década de 1970, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), já preocupada com a regulação do tráfego de dados entre diferentes países, organizou um grupo de estudos a fim de estabelecer normas referentes ao tráfego internacional. A partir disso, foram geradas as *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, em 1980. Tal documento tem como protagonista o tráfego de dados transfronteiriço, mais do que a proteção da pessoa, e serviu como fundamento para diversas legislações dos países-membros da OCDE.

A chamada Convenção 108 tratava-se da Convenção para a Proteção de Indivíduos com Respeito ao Processamento de Dados Pessoais realizada em 1981 por iniciativa do Conselho Europeu<sup>38</sup>, que entendia a proteção de Dados como assunto de Direitos Humanos. A convenção buscava incentivar os países membros do Conselho Europeu, bem como outros signatários como Argentina, México e Uruguai (para citar latino-americanos) a criar leis e normativas internas que protegessem os dados e regulassem seu processamento.

A Diretiva 95/46/CE veio padronizar a proteção de dados pessoais no contexto da União Europeia. Ela tinha por objetivo criar condições para que os dados pessoais pudessem circular livremente entre os países do bloco, facilitando as relações econômicas entre eles. Não obstante, preocupava-se também com a criação de mecanismos que tutelassem o respeito à pessoa e aos seus dados de forma a garantir seus direitos da personalidade e sua capacidade de se

---

<sup>38</sup> *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 108/1981. Também conhecida como Convenção de Strasbourg.

autodeterminar através do controle de seus dados. Conforme assinala Laeber (2007, p.8), não se escolheu na normativa a proibição da circulação dos dados, mas uma circulação “*responsável, com o respeito aos direitos individuais, haja vista que em algumas situações a circulação é muito mais favorável aos interesses dos cidadãos do que o seu bloqueio*”.<sup>39</sup>

Conforme seus 71 considerandos<sup>40</sup>, a Diretiva 46 do Parlamento e do Conselho Europeu se propunha a assegurar o progresso econômico e social através da circulação livre dos dados, mas sempre com respeito “*às liberdades e aos direitos fundamentais das pessoas independentemente da sua nacionalidade ou da sua residência, especialmente a vida privada*” (DE LUCCA; MACIEL, 2020).<sup>41</sup>

Mais tarde, em 2016, houve na Europa a aprovação do General Data Protection Regulation (GDPR) - Regulamento Geral sobre a Proteção de Dados<sup>42</sup>, que entrou em vigor em 2018, tendo eficácia em todos os países membros do bloco econômico. Trata-se de um documento com as nuances determinadas através da evolução dos debates sobre da proteção de dados ao longo dos anos.

## 1.6 Princípios da proteção de dados

Como assinala Doneda (2019, p.180), estudos realizado nos Estados Unidos vários anos antes da decisão do tribunal alemão, durante discussões acerca da criação de um imenso banco de dados sobre os cidadãos norte-americanos por parte do governo – chamado *National Data Center*, que não chegou a ser estabelecido – e a *Secretary for Health, Education and Welfare*, chegaram a conclusões acerca de premissas a serem observadas nas atividades de processamento de dados a fim de garantir os direitos dos indivíduos que tinham seus dados tratados<sup>43</sup>.

<sup>39</sup> LAEBER, Márcio Rafael Silva. Proteção de Dados Pessoais: O Direito à Autodeterminação Informativa. *Revista de Direito Bancário e do Mercado de Capitais*, v. 37, jul-set 2007. p. 8.

<sup>40</sup> Uma espécie de exposição de motivos da normativa.

<sup>41</sup> DE LUCCA, Newton; MACIEL, Renata Mota. A Proteção de Dados Pessoais no Brasil a partir da Lei 13.709/2018: Efetividade?, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital – Direito Privado e Internet*. 3.ed. Indaiatuba, SP: Editora Foco, 2020. p. 215.

<sup>42</sup> REGULAMENTO (UE) 2016/679.

<sup>43</sup> “- Não deve existir um sistema de armazenamento de informações pessoais cuja existência seja mantida em segredo. - Deve existir um meio para um indivíduo descobrir quais informações a seu respeito estão contidas em um registro e de qual forma ela é utilizada. - Deve existir um meio para um indivíduo evitar que a informação



Era possível observar, tanto nos estudos norte-americanos, quanto nas normativas advindas da iniciativa do OCDE e do Conselho Europeu, que havia um “núcleo comum” a ser observado nos processos de tratamento de dados que norteava as disposições de tais documentos. O referido autor, em sua obra, apresenta uma síntese desses princípios básicos, que foram observados em diversas leis, inclusive as de primeira geração, até as mais recentes:

- a) **Princípio da publicidade (ou da transparência)**, pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;
- b) **Princípio da exatidão**: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;
- c) **Princípio da finalidade**, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);
- d) **Princípio do livre acesso**, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;
- e) **Princípio da segurança física e lógica**, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.<sup>44</sup>

Estes princípios foram utilizados com o passar dos anos em diversas leis nacionais e normativas internacionais que tratavam da proteção de dados pessoais e até hoje fundamentam as regras e normas acerca do processamento de dados.

Ao longo do tempo, foram surgindo outros princípios através dos estudos desenvolvidos acerca da proteção de dados e da necessidade de se ter uma eficácia da garantia dos direitos dos titulares de dados. Surgiram, por exemplo, princípios relacionados à boa-fé, à adequação, à necessidade, à limitação da conservação, à qualidade dos dados, entre outros.

---

a seu respeito colhida para um determinado fim seja utilizada ou disponibilizada para outros propósitos sem o seu conhecimento. - Deve existir um meio para um indivíduo corrigir ou retificar um registro de informações a seu respeito. - Toda organização que estruture, mantenha, utilize ou divulgue registros com dados pessoais deve garantir a confiabilidade destes dados para os fins pretendidos e deve toar as devidas precauções para evitar o mau uso destes dados.” Enunciados em 1973, nos EUA.

<sup>44</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 181 – 182.

No GDPR, após todo o desenvolvimento europeu de uma cultura de proteção de dados desde, principalmente a Diretiva 95, os princípios relativos ao tratamento de dados pessoais foram elencados no Capítulo II, artigo 5º:

Artigo 5.o Princípios relativos ao tratamento de dados pessoais

1. Os dados pessoais são:

- a) Objeto de um tratamento lícito, leal e transparente em relação ao titular dos dados («**licitude, lealdade e transparência**»);
  - b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais, em conformidade com o artigo 89.o, n.o 1 («**limitação das finalidades**»);
  - c) Adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados («**minimização dos dados**»);
  - d) Exatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora («**exatidão**»);
  - e) Conservados de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são tratados; os dados pessoais podem ser conservados durante períodos mais longos, desde que sejam tratados exclusivamente para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, em conformidade com o artigo 89.o, n.o 1, sujeitos à aplicação das medidas técnicas e organizativas adequadas exigidas pelo presente regulamento, a fim de salvaguardar os direitos e liberdades do titular dos dados («**limitação da conservação**»);
  - f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação accidental, adotando as medidas técnicas ou organizativas adequadas («**integridade e confidencialidade**»);
2. O responsável pelo tratamento é responsável pelo cumprimento do disposto no n.o 1 e tem de poder comprová-lo («**responsabilidade**»).

A LGPD, por sua vez, traz seus princípios elencados no artigo 6º:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a **boa-fé** e os seguintes princípios:

- I - **finalidade**: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- II - **adequação**: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- III - **necessidade**: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- IV - **livre acesso**: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- V - **qualidade dos dados**: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - **transparência**: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - **segurança**: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - **prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - **não discriminação**: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - **responsabilização e prestação de contas**: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Assim, pode-se perceber que aqueles princípios que definiam a essência da proteção de dados há algumas décadas permanecem tendo grande importância quando se fala da garantia de um processamento de dados que respeite a dignidade humana e a capacidade do indivíduo de se autodeterminar perante a sociedade.

Ainda que com termos diferentes (como é o caso da “minimização” no GDPR e da “adequação” na LGPD), os princípios se fazem presentes nos mais diversos diplomas legais de proteção de dados, normalmente em um artigo que elenca o que deve nortear a aplicação das normas que aquela legislação prevê.

## 2. A PROTEÇÃO DE DADOS NO BRASIL

### 2.1 O *Habeas Data*

O *Habeas Data* é um instituto originário do ordenamento brasileiro após a redemocratização do país com o fim da ditadura militar. É um instrumento que foi pensado para reparar os abusos cometidos no período anterior com o uso indevido e autoritário da informação pelos que detinham o poder.

Por conta da semelhança de experiência entre os países latino-americanos na segunda metade do século XX com regimes bem restritivos e baseados nas forças militares, tal instituto foi “exportado” para outros países, cuja sociedade civil também guardava o trauma de um regime totalitário.

Em tais regimes, a informação que se tinha sobre uma pessoa era utilizada indiscriminadamente pelo poder público para ações de repressão a manifestações contrárias aos governos. Um Estado de permanente vigilância, que reprimia ações e pessoas que se opunham à forma como era governado o país e, assim, garantia a manutenção do poder. As liberdades individuais de expressão e associação eram suprimidas caso se mostrassem contrárias às ideias políticas dos que estavam no comando.

O instrumento, inaugurado na Constituição de 1988, prevê a possibilidade de o indivíduo requerer informações a seu respeito que estejam em posse das autoridades públicas. Através dele, o indivíduo poderia acessar as informações sobre ele constantes nos arquivos do poder público e, caso contassem com incoerências, corrigi-los.

Assim, prevê a Constituição Federal em seu artigo 5º:

LXXII - conceder-se-á *habeas data*:

- a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
- b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo

Danilo Doneda (2019, p. 270) comenta sobre o *Habeas Data*:

O instituto do *habeas data* foi introduzido pela Constituição brasileira de 1988, em seu artigo 5.º LXXII. Seu caráter e seu próprio *nomen iuris* são devidos a José Afonso da Silva e já estavam presentes no Projeto de Constituição elaborado pela Comissão Provisória de Estudos Constitucionais (conhecida como Comissão Afonso Arinos) A expressão *habeas data* foi pinçada por José Afonso da Silva, responsável por esta parte do projeto, da obra do espanhol Firmín Morales Prat; no entanto não é este o seu autor, visto que Vittorio Frosini já a havia utilizado, talvez com ineditismo, em 1981. Frosini, após identificar uma "liberdade informática", ou seja, uma extensão da liberdade pessoal como exigência imposta pelo desenvolvimento tecnológico, alude à importância do *habeas corpus* para a liberdade pessoal e acrescenta que: "poder-se-ia dizer, com uma paráfrase de caráter metafórico, que na legislação dos Estados modernos é necessário hoje um *habeas data*, um reconhecimento do direito do cidadão de dispor dos próprios dados pessoais, assim como ele tem o direito de dispor livremente do próprio corpo". Note-se ainda que Stefano Rodotà, em 1973, fez menção ao direito de acesso como um *habeas scriptum* - que seria um sinônimo para o *habeas data*.<sup>45</sup>

Nota-se que é um instituto que preserva a autodeterminação informativa já que reconhece que o simples fato de o Estado armazenar informações sobre os indivíduos, que possibilitam

<sup>45</sup>

Ibidem. p. 270.

identificar os mesmos, e processá-las para uma finalidade específica pode afetar a esfera de direitos do titular das informações, principalmente sendo tal finalidade muitas vezes a de perseguição política.

Ainda que date da década de 1980, por conta de uma distância tecnológica entre os países latino-americanos e os europeus, bem como os Estados Unidos, a criação do *Habeas Data* não sofreu tanta influência das normativas desses locais, que já estavam em um estágio avançado de desenvolvimento graças à informatização do processamento ter acontecido há mais tempo. É possível, entretanto, notar que há reflexos dos ordenamentos de Portugal e da Espanha, que também tinham saído de regimes autoritários (DONEDA, 2020)<sup>46</sup>.

O *Habeas data*, entretanto, sendo constituído como uma ação constitucional, tem caráter de instrumento, e não de direito material. Ainda assim, é uma conquista democrática que veio a ser concebida em momento oportuno no ordenamento jurídico brasileiro. Sobre isso, Laura Mendes (2018, p. 199) ressalta que:

É certo que a doutrina há tempos já descreveu as limitações do *habeas data*, derivadas tanto da sua forma (o fato de constituir uma ação constitucional e não um direito material expresso) quanto de sua origem (instrumento concebido da passagem da ditadura para a democratização). No entanto, a despeito dessas limitações, é preciso destacar a modernidade desse instrumento, na medida em que ele reconhece a informação pessoal como um objeto merecedor de proteção constitucional.<sup>47</sup>

No entanto, há que se ressaltar que a ideia original do instituto quando foi proposta seria uma proteção expressa de direitos comuns às legislações de proteção de dados, conforme relata Danilo Doneda (2019, p. 272):

O *habeas data* é um produto de seu tempo: tendo nascido como remédio para um problema específico, conforme mencionamos, enfrenta o desafio de demonstrar sua aplicabilidade e eficácia em situações bastante diversas. Voltando ao momento da sua instituição, vemos que o constituinte brasileiro optou por não estabelecer um sistema de garantias individuais expressas positivamente, integrando o direito de acesso, retificação e outros com a principiologia relacionada a proteção de dados pessoais.

---

<sup>46</sup> Ibidem. p. 269.

<sup>47</sup> MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

Preferiu a técnica de reconhecer tais direitos por meio de uma ação voltada a sua defesa - aliás, em oposição ao teor do Projeto da Comissão Afonso Arinos.<sup>48</sup>

Por ter sido inaugurado na legislação brasileira através de uma ação<sup>49</sup> e ter requisitos específicos, sua utilização acabou muitas vezes por ser limitada. A incidência deste quanto a bancos de dados de “caráter público” gerou bastante debate, pois por um tempo entendia-se que tal termo restringia a aplicação somente a bancos de dados da administração pública. Superada, parcialmente, tal questão, através de atuação da doutrina, ainda havia dificuldade em uma ampla utilização por parte dos indivíduos.

O “interesse de agir” e o “esgotamento das vias administrativas”, requisitos exigidos através da interpretação do STF do referido instituto acabam por ser os maiores empecilhos para que tal instrumento possa ser utilizado mais amplamente. Demonstrar tais requisitos demanda muito tempo e esforço por parte do interessado.

Além disso, para interpor um *Habeas Data*, é necessário o patrocínio de um advogado (diferente do que é exigido para o *Habeas Corpus*, por exemplo), o que se entende ser desproporcional à proteção que o instituto visa tutelar.

Entretanto, Mendes (2018, p. 203) faz questão de assinalar que, com o advento da LGPD no ordenamento brasileiro, o *habeas data* pode ser mais amplamente utilizado:

Com o reconhecimento de um direito material de proteção de dados pessoais na Constituição Federal, abrem-se novas possibilidades para o desenvolvimento dessa ação, de modo a permitir um entendimento de sua aplicação compatível com a importância da proteção de dados pessoais na atual sociedade da informação. Sob essa perspectiva, entende-se que as hipóteses previstas no art. 5.º, LXXII, da CF/1988 – acesso, retificação e complementação dos dados – são apenas algumas das formas processuais de proteção da privacidade, não esgotando todos os instrumentos constitucionais de tutela.<sup>50</sup>

<sup>48</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 272.

<sup>49</sup> Sobre isso: “O direito do indivíduo de que o tratamento de dados pessoais que lhe digam respeito seja objeto de um tratamento leal, para fins específicos e com o consentimento do indivíduo ou com outro fundamento legítimo previsto por lei. A efetivação desse direito depende ainda da fiscalização por uma autoridade independente e que sejam garantidas a pretensão de acesso a esses dados, de retificação e de cancelamento em caso de tratamento ilegal, garantias essas que compõem o instrumento do *habeas data*”. BRITZ, Gabriele. *Freie Entfaltung durch Selbstdarstellung*. Tübingen: Mohr Siebeck, 2007. p. 169. apud MENDES, Laura Schertel Ferreira. *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*. Direitos Fundamentais & Justiça, Belo Horizonte, ano 12, n. 39, jul./dez. 2018. p. 205.

<sup>50</sup> MENDES, Laura Schertel Ferreira. *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, jul./dez. 2018. p. 203.

Mais que isso, como se tratam de “dois lados da mesma moeda”, pelo fato de um ser “*uma garantia processual de proteção das liberdades e da personalidade frente ao tratamento de dados*” e o outro um “*direito material propriamente dito, que protege o indivíduo dos riscos decorrentes desse processamento*”<sup>51</sup>, o *habeas data* pode ser reinterpretado de forma a garantir a autodeterminação informativa como um direito constitucionalmente protegido. A proteção de dados passa a figurar como direito fundamental “*amparada na inviolabilidade da intimidade e da vida privada e da dignidade humana*”<sup>52</sup>.

Nesse sentido, pode-se citar o RE nº 673.707, oriundo de Minas Gerais, relatado pelo Min. Luiz Fux em 17.06.2017 que destacou que:

Em primeiro lugar, o relator acabou por atribuir um amplo espectro de proteção ao *habeas data* a partir de um amplo conceito de arquivos, banco ou registros de dados “entendidos em seu sentido mais lato, abrangendo tudo que diga respeito ao interessado, seja de modo direto ou indireto.”

(...)

aos contribuintes foi assegurado o direito de conhecer as informações *que lhes digam respeito em bancos de dados públicos ou de caráter público*, em razão da necessidade de *preservar o status de seu nome, planejamento empresarial, estratégia de investimento e, em especial, a recuperação de tributos pagos indevidamente, dentre outras*. Consectariamente, estas informações não são de uso privativo do órgão ou entidade produtora ou depositária das informações, a Receita Federal do Brasil, *mas dizem respeito ao próprio contribuinte*.<sup>53</sup>

Laura Mendes (2018, p. 214) entende que por conta de alguns aspectos é que se deve afirmar a necessidade de reinterpretar o instituto do *habeas data* de forma a garantir a proteção de dados como um direito fundamental protegido pelo texto constitucional, sendo eles:

a) a dependência dos indivíduos em relação à infraestrutura de comunicação e informação; b) os riscos individuais que o processamento e a utilização de informação podem causar; c) a influência do processamento e da utilização de informações no sistema de direitos fundamentais como um todo; e d) a ineficácia de um sistema de proteção *ex post*, baseado meramente na reparação de danos.<sup>54</sup>

<sup>51</sup> Ibidem. p. 197-198.

<sup>52</sup> Ibidem. p. 201.

<sup>53</sup> RE nº 673.707

<sup>54</sup> MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, jul./dez. 2018. p. 214.

## 2.2 O Código de Defesa do Consumidor

O Código de Defesa do Consumidor (Lei nº 8.078) foi promulgado em 1990, trazendo as primeiras normas sobre a regulação dos bancos de dados em solo brasileiro. O principal dispositivo que tutela tal questão é o artigo 43:

Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

§ 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.

§ 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.

§ 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.

§ 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

§ 5º Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

§ 6º Todas as informações de que trata o caput deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor.

Como o CDC rege as formas de consumo de forma ampla, o dispositivo alcança todo e qualquer dado pessoal do consumidor. As disposições consumeristas visam reequilibrar as relações entre o fornecedor e o consumidor, de maneira a capacitar o consumidor para autodeterminar as suas informações pessoais (BIONI, 2020)<sup>55</sup>.

Também Doneda (2019, p. 266) comenta o foco do Código de Defesa do Consumidor:

As disposições do CDC revelam, como foco de preocupação do legislador, o estabelecimento de equilíbrio na relação de consumo por meio da interposição de limites ao uso da informação sobre o consumidor pelo fornecedor (que estaria justificado, de certo ponto de vista, na efetivação da transação com maior segurança). Assim, por exemplo, o registro de dados negativos sobre um consumidor não poderá ser mantido por um período maior de 5 anos; é prevista a necessidade de comunicação escrita sobre o tratamento da informação ao consumidor em certos casos, assim como o direito de acesso, correção e implicitamente, o cancelamento justificado.<sup>56</sup>

<sup>55</sup> BIONI, Bruno. *Proteção de Dados Pessoais – A Função e os Limites do Consentimento*. 2. ed. Rio de Janeiro: Forense, 2020. p. 121.

<sup>56</sup> DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 266.



Nota-se, assim, um protagonismo da transparência como forma de garantir ao consumidor o controle de seus dados. É claro na disciplina de Direito do Consumidor que a informação tem papel de importante relevância na garantia do consumidor em ser preservado dada sua vulnerabilidade ante ao fornecedor, sem informação adequada e clara não há tomada de decisões plenamente consciente.

É por tal proteção que se garante, por exemplo, a necessidade de que o consumidor deve sempre ser informado quando da inclusão de suas informações em bancos de dados. Além disso, também consta no caput do artigo 43 o direito de acesso dos consumidores às informações constantes nos bancos de dados decorrentes de suas relações consumeristas, através da manutenção desse direito, permite-se também ao consumidor que possa alterar dados errôneos, através do direito de retificação a fim de velar pela exatidão dos dados e, conseqüentemente, pela identidade do consumidor, atendendo a necessidade da qualidade do tratamento.

Outro direito importante também garantido pelo CDC no tocante ao processamento de dados pessoais é a limitação temporal pela qual os dados negativos, isto é, aqueles relacionados à inadimplências, só podem ser armazenados e considerados por cinco anos. Pode, por fim, o consumidor cancelar o processamento de seus dados incorretos ou que já tenham alcançado o limite temporal.

### **2.3 A Lei do Cadastro Positivo**

No Brasil, o cadastro de maus pagadores foi implantado tardiamente, cerca de 100 anos após terem sido iniciados em países como a Inglaterra e os Estados Unidos. Antes disso, para se conceder crédito aos indivíduos, os lojistas mantinham relações diretas entre si, o que tornava o processo muito mais lento.

Em 1955, surgiu o primeiro banco de dados negativo (com informações de inadimplência) do Brasil, o Serviço de Proteção ao Crédito (SPC). Em 1968, surgiu a Centralização dos Serviços de Bancos (Serasa). Em âmbito público, tem-se como protagonistas o Cadastro de Emitentes de Cheques sem Fundos do Banco do Brasil e o Cadastro Informativo de Créditos não Quitados no Setor Público Federal (Cadim).

O fato de haver apenas informações negativas nestes bancos de dados, isto é, relativas a inadimplimentos, trouxe problemas a quem tinha bons históricos de pagamento, pois deles nada havia de informação nos bancos de dados.

O Cadastro Positivo, foi inaugurado no Brasil a partir da Lei 12.414, de 9 de junho de 2011. Até então, o Brasil, que tem um sistema de crédito pequeno, tinha basicamente bancos de dados de informações negativas sobre os hábitos de pagamento dos cidadãos, contendo as informações apenas de maus pagadores. Através da referida lei, visando a concessão de crédito, começou-se a incluir informações das pessoas que tinham bons históricos de pagamento, por isso o nome “cadastro positivo”.

Com uma série de movimentos legislativos (MP 518/2010; Lei 12.414/2011; Decreto 7.829/2013 e a Resolução do Banco Central n. 4.172) foi-se instaurando um sistema de cadastro positivo no Brasil. Através deste permitiu-se ao consumidor fornecer informações positivas de seu histórico de pagamento e regrou-se a utilização por parte dos interessados.

A Lei do Cadastro Positivo, trouxe, para regular a utilização das informações dos bons pagadores, 4 figuras que participarão deste processo. O cadastrado é o consumidor que autoriza a inclusão de suas informações no banco de dados; o gestor é aquele responsável pela coleta, armazenamento, análise do banco de dados; a fonte é quem concede crédito ou pratica transações que tenham risco financeiro; e o consulente é quem acessa as informações constantes no banco de dados para seus fins permitidos em lei.

Além disso, o sistema de regulação desse Cadastro Positivo também se preocupou em descrever quais informações de pagamento podem constar no cadastro de bons pagadores, a forma como podem ser utilizadas, bem como quais informações não podem ser coletadas, como dados sensíveis por exemplo. Tudo isso para melhorar as relações do sistema financeiro e incentivar seu aumento.

A teoria da informação assimétrica ajuda a entender certas dificuldades de estabilidade do mercado de crédito. Por ela, entende-se que em determinadas situações uma das partes detém mais informações que outra, como na concessão de empréstimos e financiamentos. Com a falta de informações para os bancos de dados que fundamentam as tomadas de decisão quanto à concessão de crédito, a análise de risco nessas concessões se

torna muito imprecisa, pois torna-se mais difícil diferenciar bons e maus tomadores. Em seguida, as taxas de juros começam a crescer, afastando os bons pagadores. A incerteza faz com que seja inviável os empréstimos e concessões a indivíduos dos quais não se tem informações de pagamento (BARCELLOS e BARCELLOS, 2017).<sup>57</sup>

O Cadastro positivo se apresenta, assim, como um instrumento para minimizar as distorções nas relações de concessão de crédito, valorizando quem mantém seus compromissos de pagamento. Ele pode ser enquadrado como uma “sinalização”, um mecanismo utilizado para evidenciar ao mercado suas características. A partir do momento que se conhece um bom histórico de pagamentos de um indivíduo, é possível literalmente “dar crédito” a sua fama de bom pagador e impor-lhe menores taxas para que este fique mais à vontade para tomar tais serviços. Isso leva a uma segurança maior das transações, que normalmente apresentam um risco, e pode levar a uma ampliação do mercado. A dificuldade, porém, está em que as pessoas se sintam de fato motivadas a fornecer suas informações para um cadastro positivo.

Como havia a lacuna na lei de quanto tempo as informações do novo cadastro estariam disponíveis (o cadastro negativo eram 5 anos, de acordo com o CDC), também havia uma desvantagem técnica. Além disso, a necessidade do cadastrado de judicializar qualquer questão relacionada a abusos configurava uma vulnerabilidade jurídica.

Num julgamento sobre a aceitação do cadastro positivo no STJ<sup>58</sup> observou-se que: 1. O Sistema de *credit score* é lícito, autorizado pelo art 5º, IV e 7º, da Lei do Cadastro Positivo. 2. Os limites referentes à privacidade e à transparência do sistema de proteção ao consumidor devem ser observados na avaliação do risco de crédito. 3. Ainda que não se precise de autorização para a inclusão de suas informações, o consumidor tem o direito ao esclarecimento das fontes dos dados. 4. Desrespeitos aos limites legais configuram abuso de direito e podem ensejar responsabilidade por danos morais ao consumidor.

---

<sup>57</sup> BARCELLOS, Daniela Silva Fontoura; BARCELLOS, Tatiana Silva Fontoura. O Cadastro Positivo no Brasil: Uma análise empírica a partir dos casos julgados do Superior Tribunal De Justiça. *Revista de Direito, Economia e Desenvolvimento Sustentável*. v. 3, n.1, p. 52-73. Brasília, jan./jun. 2017.

<sup>58</sup> REsp 1419697/RS.

A reputação passa a ser utilizada como garantia dos empréstimos e financiamentos e, conforme observado por Barcellos e Barcellos (2017, p. 71), em países que detém um sistema positivo e negativo de histórico de pagamentos, isto tende a melhorar a economia. Com a aceitação, por parte do judiciário, dos sistemas de cadastro positivos, consolida-se uma segurança jurídica na aplicação das análises de crédito que se utilizem de informações de adimplemento.<sup>59</sup>

## 2.4 A Lei de Acesso à Informação

A Lei de Acesso à Informação (Lei 12.527 – LAI) foi aprovada em 2011 e veio para regular o direito fundamental disposto no artigo 5º, inciso XXXIII da Constituição Federal: *“todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado”*.

A lei objetiva assegurar aos cidadãos o direito de obter informações de interesse particular, coletivo ou geral dos órgãos públicos. Assim, traz um conjunto de diretrizes para a regulação do acesso a informações em poder dos entes públicos:

Art. 3º Os procedimentos previstos nesta Lei destinam-se a assegurar o direito fundamental de acesso à informação e devem ser executados em conformidade com os princípios básicos da administração pública e com as seguintes diretrizes:

- I - observância da publicidade como preceito geral e do sigilo como exceção;
- II - divulgação de informações de interesse público, independentemente de solicitações;
- III - utilização de meios de comunicação viabilizados pela tecnologia da informação;
- IV - fomento ao desenvolvimento da cultura de transparência na administração pública;
- V - desenvolvimento do controle social da administração pública.

O valor prático que tais diretrizes apresentam é que a transparência é a regra quando se falam das informações da administração pública, sendo o sigilo a exceção. A lei tem por centro a garantia do acesso pleno às informações.

---

<sup>59</sup> BARCELLOS, Daniela Silva Fontoura e BARCELLOS, Tatiana Silva Fontoura. O Cadastro Positivo no Brasil: Uma análise empírica a partir dos casos julgados do Superior Tribunal De Justiça. *Revista de Direito, Economia e Desenvolvimento Sustentável*. v. 3, n.1, p. 52-73. Brasília, jan./jun. 2017.

Interessante destacar que, ainda que tendo por pressuposto a efetividade da transparência pública, a LAI já tinha exceções quanto às informações pessoais, como se destaca no artigo 31 da lei:

Art. 31. O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.

§ 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem:

I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e

II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

§ 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido.

§ 3º O consentimento referido no inciso II do § 1º não será exigido quando as informações forem necessárias:

I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III - ao cumprimento de ordem judicial;

IV - à defesa de direitos humanos; ou

V - à proteção do interesse público e geral preponderante.

§ 4º A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

§ 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal.

Ainda que o acesso à informação pública seja a regra, nota-se a preocupação do legislador em proteger dados e informações pessoais dispostos em bancos de dados públicos. Observa-se que a lei coloca como valores importantes para o tratamento de dados pessoais pelo poder público a intimidade, a vida privada, a honra e a imagem das pessoas, além das liberdades e garantias individuais.

Cria assim uma restrição de acesso, conforme o art. 31, § 1º, I, bem como regras para a divulgação dos dados pessoais à terceiros no § 1º, inciso II e os incisos do § 3º, impondo a necessidade de consentimento ou do atendimento de algumas hipóteses específicas.

Ana Carla Harmatiuk Matos e Carlos Eduardo Ruzyk (2019, p. 199-218) destacam, entretanto, que a lei não é precisa quanto a quais dados precisam efetivamente do consentimento para serem tratados, principalmente por conta do conceito de interesse público:

A Lei de Acesso à Informação, em seu artigo 31, contém comando que impõe, no tratamento de dados pessoais, a transparência frente ao seu titular, bem como o respeito ‘à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdade e garantias individuais’.

Entre os dados pessoais, o § 1º destaca aqueles que seriam, na *ratio* desse diploma legal, relativos à intimidade, vida privada, honra e imagem, os quais são reputados de acesso exclusivo a agentes públicos legalmente autorizados e ao seu próprio titular, e cujo conhecimento por terceiros depende, em regra, de autorização do titular – salvo as exceções enumeradas no § 3º, que dispensam a autorização.

A rigor, o que emerge desses comandos normativos, é uma restrição ao acesso a determinados dados pessoais – sem, porém, uma criteriosa distinção que especifique quais seriam tais dados especialmente protegidos, e quais seriam aqueles de amplo acesso e tratamento.

A referência à vida privada não é bastante, uma vez que a própria autodeterminação informativa – que, *prima facie*, se refere, genericamente, a quaisquer dados pessoais, e não apenas a dados sensíveis (dados especialmente protegidos pela Lei, como os dados relativos à origem étnica ou vinculados à saúde e dados biométricos) – integra o âmbito de proteção da vida privada.

Evidencia-se a insuficiência da Lei de Acesso à Informação para a delimitação de quais dados pessoais se sujeitam, efetivamente, a consentimento para o seu tratamento.

A dúvida que sempre esteve presente desde a vigência da Lei de Acesso à Informação foi, mesmo, sobre o que se pode compreender como dados pessoais, e, entre estes, quais podem ser considerados públicos – sendo que a própria anonimização de dados e sua divulgação se apresentava como passível de controvérsia.<sup>60</sup>

Importante ressaltar também, que a LAI tutela o acesso às informações de bancos de dados públicos, não se aplicando às demais relações concernentes ao processamento de dados pessoais.

## 2.5 A Lei Geral de Proteção de Dados

A LGPD, Lei 13.709 de 14 de agosto de 2018, teve sua aprovação impulsionada principalmente pelo movimento europeu de normatização e padronização do tratamento de dados. Assim, quando em maio daquele ano, o GDPR (que havia sido aprovado 2 anos antes) começou sua vigência, trazendo normas que beneficiavam as relações econômicas entre países

<sup>60</sup> MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à informação. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 199-218.

com proteção de dados considerada de nível satisfatório, o Brasil viu-se na urgência em aprovar o diploma, que já era debatido há anos no Congresso.

Ainda que já houvesse no ordenamento jurídico brasileiro diversos dispositivos que versavam sobre a proteção de dados pessoais, faltava ainda uma lei específica que regulamentasse a utilização das informações por parte dos interessados e os direitos que deveriam ser reconhecidos aos titulares.

O PL havia sido proposto em 2012 na Câmara dos Deputados (Projeto de Lei 4.060/12) e com a ocorrência dos casos internacionais de vazamentos de dados e o “atraso” numa regulação mais assertiva de tais questões, entrou em regime de urgência para ser aprovada na Câmara dos Deputados e no Senado e sancionada pela Presidência em agosto de 2018. Meses depois, a Medida Provisória 869/2018, editada pelo então presidente Michel Temer no “apagar das luzes do governo”, alterou alguns aspectos da lei e disciplinou a criação da Autoridade Nacional de Proteção de Dados.

Sobre a importância da LGPD para a proteção de dados no Brasil, comentam Danilo Doneda e Laura Mendes (2018, p. 25):

A lei aprovada proporciona ao cidadão garantias em relação ao uso dos seus dados, a partir de princípios, de direitos do titular de dados e de mecanismos de tutela idealizados tanto para a proteção do cidadão quanto para que o mercado e setor público possam utilizar esses dados pessoais, dentro dos parâmetros e limites de sua utilização. Esta é uma experiência que vem se mostrando exitosa em diversos outros países, introduzindo o paradigma do controle – pelo qual se garante ao cidadão o controle sobre seus dados, inclusive para que os divulgue e use, em oposição ao paradigma do segredo e do sigilo.<sup>61</sup>

Vale ressaltar, que a tramitação da LGPD no Congresso se deu por um amplo debate entre vários setores da sociedade<sup>62</sup>. Assim, houve participação, por exemplo, do setor econômico, das

---

<sup>61</sup> MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): O novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555-587, nov./dez. 2018.

<sup>62</sup> Os mesmos autores comentam que “A partir de um processo democrático realizado na internet e de forma muito semelhante ao debate público do Marco Civil da Internet, as consultas públicas realizadas em 2010 e 2015 resultaram em um total de quase 2.000 contribuições da sociedade civil, especialistas, órgãos do governo e empresas. Em 2016, o Projeto foi enviado à Câmara dos Deputados e passou a tramitar em paralelo com Projeto de Lei do Senado sobre o mesmo tema (PLS 330/2013). Na Câmara dos Deputados, foi criada a Comissão Especial de Proteção de Dados Pessoais e designado como relator o Deputado Orlando Silva, que, após uma série de audiências públicas, seminários e reuniões intersetoriais, conduziu a matéria para a sua aprovação por unanimidade

associações de direitos dos consumidores, do setor de tecnologia e de muitos especialistas de diversas áreas, garantindo assim uma construção conjunta, que levava em conta vários interesses. Observa-se, então, que a LGPD se apresenta não como uma lei que visa proibir a utilização dos dados pessoais, nem tampouco uma lei que desconsidere a centralidade da proteção no indivíduo e no livre desenvolvimento de sua personalidade.

A Lei Geral de Proteção de Dados visa garantir um processamento de dados que não viole a capacidade de autodeterminação informativa do indivíduo, sem deixar de estimular o crescimento econômico através das atividades de tratamento, conforme pode-se depreender de seus fundamentos:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:

I - o respeito à privacidade;

II - a autodeterminação informativa;

III - a liberdade de expressão, de informação, de comunicação e de opinião;

IV - a inviolabilidade da intimidade, da honra e da imagem;

V - o desenvolvimento econômico e tecnológico e a inovação;

VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

### 2.5.1 O conceito de dado pessoal

A Lei 13.709 traz em seu artigo 5º, inciso I, como seria esperado numa normativa que se focasse na proteção de dados pessoais, a definição de dado pessoal como sendo uma *“informação relacionada a pessoa natural identificada ou identificável”*.

Trata-se de um conceito curto, que foi o resultado de anos de debates legislativos acerca da questão da definição de dados pessoais, já que, a partir dela é que se pode enxergar o espectro de alcance da proteção legal.

Faz-se mister, entretanto, citar que no Anteprojeto de lei, ainda em 2011, era apresentado um conceito um pouco maior no artigo 4º, inciso I: *“qualquer informação relativa a uma pessoa determinada ou identificável, direta ou indiretamente, incluindo todo endereço ou número de identificação de um terminal utilizado para conexão a uma rede de computadores”*.

---

em plenário. Em seguida, por meio da relatoria do Senador Ricardo Ferraço, o PLC 53/2018 foi aprovado por unanimidade também no Senado Federal”.



Já o Anteprojeto de Lei sobre Proteção de Dados de 2015, previa no artigo 5º, I, em sua primeira versão que dado pessoal é *“dado relacionado a pessoa natural determinada ou determinável, inclusive a partir de números identificativos, dados locacionais ou identificadores eletrônicos”*, e na segunda versão: *“dado relacionado a pessoa natural determinada ou determinável inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa”*. Percebe-se que em tais conceitos, já havia uma restrição à pessoa natural.

Em 2013, no Projeto de Lei nº 330 do Senado Federal, o dado pessoal era descrito como *“toda informação, de qualquer natureza e independentemente do respectivo suporte, passível de ser armazenada, processada ou transmitida, relativa pessoas identificadas ou identificáveis”*. Tal conceito foi um pouco alterado com a emenda 31 – CCT/CMA e resultou no conceito de dado pessoal como sendo *“qualquer informação referente a pessoa natural identificável ou identificada”*. Este último, com a alteração de “referente” para “relacionada”, foi o que prevaleceu até a aprovação da LGPD.

Observa-se, assim, que se optou por uma descrição mais sucinta, mas que não deixa de abranger as especificidades citadas nos conceitos anteriormente propostos. Há, entretanto, parte da Doutrina, que critica a definição adotada, por restringir o dado pessoal, e consequentemente a proteção conferida pela lei às pessoas naturais.

Newton de Lucca e Renata Mota Maciel (2020, p. 222), defendem que a restrição da proteção às pessoas naturais não se justifica no *“cenário atual em que os meios tecnológicos são instrumentos para o desenvolvimento como um todo, incluídas nessa ideia não apenas as pessoas naturais, como também as jurídicas”*<sup>63</sup>. Também apoia tal posição Cíntia Rosa Pereira de Lima.

Há que se perceber, entretanto, que a definição adotada pelo GDPR, ainda que maior e mais descritiva, também restringe o titular à pessoa natural:

---

<sup>63</sup> DE LUCCA, Newton; MACIEL, Renata Mota. A Proteção de Dados Pessoais no Brasil a partir da Lei 13.709/2018: Efetividade?, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital – Direito Privado e Internet*. 3.ed. Indaiatuba, SP: Editora Foco, 2020. p. 222.

Art 4º, “1”. «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular

A preocupação quanto à proteção da capacidade de se autodeterminar informativamente era visivelmente direcionada às pessoas naturais, sujeitos de direitos relacionados à dignidade humana.

### 3. O DIREITO DE ACESSO AOS DADOS PELO TITULAR

Dado o histórico da evolução da tutela da dignidade humana em face das atividades de processamento de dados, a LGPD traz normas que visam proteger o direito ao livre desenvolvimento da personalidade do indivíduo, garantido a ele não só a proteção de sua intimidade, mas a possibilidade de se autodeterminar, de exercer o controle sobre os seus dados e sobre sua identidade.

A lei vem responder a uma preocupação real gerada pelo o amplo tratamento de dados pessoais que plasma a sociedade informacional. Sobre essa preocupação, já falava há muito o Ministro Ruy Rosado:

A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto dessa indiscriminada colheita de informações, muitas vezes, sequer sabe da existência de tal atividade, ou não dispõe de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador.<sup>64</sup>

<sup>64</sup>

STJ, Recurso Especial n. 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995.

No que tange à proteção de dados, o controle dos dados “compõe um aspecto essencial da dimensão subjetiva” deste direito (MENDES, 2018)<sup>65</sup>. Como dados pessoais tratam-se de dados relacionados à pessoa, terão forte influência sobre sua vida e direitos, logo o titular, aquele de quem as informações estão atreladas, deve ter o poder de determinar como esses dados circulam, exercendo o controle sobre a coleta, o processamento, a utilização e a transferência deles.

Sobre a necessidade de o indivíduo ter assegurado o controle sobre seus dados, fala Caitlin Sampaio Mulholland (2018, p. 172):

A ampliação do conceito de *privacy* se deu, em grande medida, por conta da evolução das formas de divulgação e apreensão de dados pessoais. Com o advento de novas tecnologias, notadamente o desenvolvimento da biotecnologia e da Internet, o acesso a dados sensíveis e, conseqüentemente, a sua divulgação, foram facilitados de forma extrema. Como resultado, existe uma expansão das formas potenciais de violação da esfera privada, na medida em que se mostra a facilidade por meio da qual é possível o acesso não autorizado de terceiros a esses dados. Com isso, a tutela da privacidade passa a ser vista não só como o direito de não ser molestado, mas também como o direito de ter controle sobre os dados pessoais e, com isso, impedir a sua circulação indesejada <sup>66</sup>

Em busca de uma tutela do titular dos dados como um indivíduo capaz de controlar seus dados, traz a LGPD, em seu artigo 18, direitos do titular:

Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:

- I - confirmação da existência de tratamento;
- II - acesso aos dados;
- III - correção de dados incompletos, inexatos ou desatualizados;
- IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
- VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei.

§ 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional.

<sup>65</sup> MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, jul./dez. 2018. p. 206.

<sup>66</sup> MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, set./dez. 2018. p. 172.

§ 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 3º Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento.

§ 4º Em caso de impossibilidade de adoção imediata da providência de que trata o § 3º deste artigo, o controlador enviará ao titular resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 5º O requerimento referido no § 3º deste artigo será atendido sem custos para o titular, nos prazos e nos termos previstos em regulamento.

§ 6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional

§ 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.

§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor.

Observando-se direitos como o de correção, anonimização, eliminação, portabilidade, revogação de consentimento, revisão de decisões, nota-se que se apresentam como meios para que o titular tenha controle sobre suas informações, à medida que o tornam participante do processo de tratamento<sup>67</sup> de seus dados. Para que tais direitos sejam plenamente exercidos, o indivíduo precisa antes saber quais dados estão em posse dos agentes de tratamento e como eles estão sendo utilizados.

É muito comum que se saiba que dados próprios são tratados pelos mais diversos agentes com que se mantém relações, sejam eles públicos ou privados. Entretanto, é notório que o indivíduo normalmente não sabe a extensão do conhecimento de empresas e outras entidades acerca de sua vida e sua personalidade.

Tal desconhecimento aumenta a disparidade de informação entre os titulares e os interessados nos dados e nas informações que decorrem do tratamento destes. A pessoa acaba muitas vezes tendo pouca ingerência sobre o que se sabe sobre ela, pois comumente, o interessado não disponibiliza esse conhecimento ao titular de forma automática.

---

<sup>67</sup> O tratamento é entendido pela LGPD como gênero que engloba diversas operações, conforme disposto em rol exemplificativo da definição do artigo 5º, inciso X: “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

Numa eventual relação em que o indivíduo fornece dados através de um formulário para uma determinada entidade, ele tem o conhecimento de quais dados estão sob a guarda daquela organização. Entretanto, imaginando que tal entidade utilizará os dados fornecidos, comparando com outros dados através de mecanismos informáticos, ela obterá conclusões acerca do tratamento realizado, que nortearão sua atividade. Assim, a partir das atividades de tratamento, os interessados têm em mãos informações e conclusões sobre os indivíduos que estes mesmos desconhecem.

Trazendo a hipótese para a realidade da sociedade da informação, onde os dados são coletados a todo momento e processados em escalas gigantescas, é impossível ao indivíduo contabilizar por si que dados cada entidade que realiza a coleta tem sobre ele, quem dirá quais informações são concluídas a partir de seus dados.

Como afirma Hoffmann-Riem (2009, apud MENDES, 2018, p. 209), a falta de conhecimento do que se sabe sobre si, leva à perda de controle sobre os dados:

Na utilização das modernas infraestruturas de comunicação, os afetados não conhecem, na maioria das vezes, o que acontece com os seus dados, quais as possibilidades de interconexão existentes na Internet e na Intranet, que chances e riscos estão relacionados a isso e que consequências futuras isso terá – como se sabe, a internet não esquece. A dimensão do problema também é caracterizada pelo fato de que o conhecimento acerca das possibilidades de uso e abuso por terceiros é limitado, assim como o conhecimento acerca de como o indivíduo pode se proteger.<sup>68</sup>

A identidade do indivíduo construída através de suas liberdades de se portar e de se revelar ao mundo exterior, acaba por ser mitigada pela identidade formada pelo que é sabido sobre ele, como relata Têmis Limberger (2020, p. 284):

O conhece-te a ti mesmo, já não é uma operação voltada ao interior, mas devido a esta nova perspectiva, vai-se ao exterior e à suposta necessidade de conhecer quem somos na dimensão eletrônica, aonde se desenvolvem questões importantes nas nossas vidas. Considerando hoje a dinâmica que caracteriza a recolhida dos dados e os sujeitos que a utilizam, cada vez é menos verossímil uma identidade como sou o que digo que sou pois que haveria que substituí-la por tu és o que Google diz que és.<sup>69</sup>

<sup>68</sup> HOFFMANN-RIEM, Wolfgang. *Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation*. *Archiv des öffentlichen Rechts*, 134, 2009. apud MENDES, Laura Schertel Ferreira. *Habeas data e autodeterminação informativa: os dois lados da mesma moeda*. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

<sup>69</sup> LIMBERGER, Têmis. Informação em Rede: Uma comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital – Direito Privado e Internet*. 3.ed. Indaiatuba, SP: Editora Foco, 2020. p. 284.

É nesse raciocínio que o Direito de Acesso, trazido no inciso II, do artigo 18 da LGPD funciona como um motor de propulsão da efetivação do controle do titular sobre os dados que circulam sobre ele. O direito é também assegurado por um princípio da proteção de dados disposto no artigo 6º, o livre acesso.

A referida autora assinala que:

o direito de acesso aos dados representa um aliado forte, em termos de proteção jurídica, que permite manter o controle sobre as próprias informações, seja qual for o sujeito que as gestiona, o local em que se encontrem e as modalidades de sua utilização. Direito fundamental a construção da identidade, já que confere poder para cancelamento nos seguintes casos dados falsos, ilegitimamente recolhidos, conservados muito além do tempo previsto, os inexatos<sup>70</sup>

O Direito de Acesso aos dados, entretanto, já era uma preocupação do legislador, desde antes da LGPD, como foi observado nas discussões acerca dos dispositivos do CDC, da LAI, da Lei do Cadastro Positivo e do *Habeas Data*.

Também o Judiciário, já reconhecia essa importância em se conhecer as informações que existem sobre si mesmo em um banco de dados, conforme destacado pela Ministra Nancy Andrighi em julgamento do STJ:

RECURSO ESPECIAL. FUNDAMENTO NÃO IMPUGNADO. SÚM. 283/STF. AÇÃO DE COMPENSAÇÃO DE DANO MORAL. BANCO DE DADOS. COMPARTILHAMENTO DE INFORMAÇÕES PESSOAIS. DEVER DE INFORMAÇÃO. VIOLAÇÃO. DANO MORAL IN RE IPSA. JULGAMENTO: CPC/15. 1. Ação de compensação de dano moral ajuizada em 10/05/2013, da qual foi extraído o presente recurso especial, interposto em 29/04/2016 e atribuído ao gabinete em 31/01/2017. 2. O propósito recursal é dizer sobre: (i) a ocorrência de inovação recursal nas razões da apelação interposta pelo recorrido; (ii) a caracterização do dano moral em decorrência da disponibilização/comercialização de dados pessoais do recorrido em banco de dados mantido pela recorrente. 3. A existência de fundamento não impugnado - quando suficiente para a manutenção das conclusões do acórdão recorrido - impede a apreciação do recurso especial (súm. 283/STF). 4. A hipótese dos autos é distinta daquela tratada no julgamento do REsp 1.419.697/RS (julgado em 12/11/2014, pela sistemática dos recursos repetitivos, DJe de 17/11/2014), em que a Segunda Seção decidiu que, no sistema credit scoring, não se pode exigir o prévio e expresso consentimento do consumidor avaliado, pois não constitui um cadastro ou banco de dados, mas um modelo estatístico. 5. A gestão do banco de dados impõe a estrita observância das exigências contidas nas respectivas normas de regência - CDC e Lei 12.414/2011 - dentre as quais se destaca o dever de informação, que tem como uma de suas vertentes o dever de comunicar

<sup>70</sup>

Ibidem.

por escrito ao consumidor a abertura de cadastro, ficha, registro e dados pessoais e de consumo, quando não solicitada por ele. 6. **O consumidor tem o direito de tomar conhecimento de que informações a seu respeito estão sendo arquivadas/comercializadas por terceiro, sem a sua autorização, porque desse direito decorrem outros dois que lhe são assegurados pelo ordenamento jurídico: o direito de acesso aos dados armazenados e o direito à retificação das informações incorretas.** 7. A inobservância dos deveres associados ao tratamento (que inclui a coleta, o armazenamento e a transferência a terceiros) dos dados do consumidor - dentre os quais se inclui o dever de informar - faz nascer para este a pretensão de indenização pelos danos causados e a de fazer cessar, imediatamente, a ofensa aos direitos da personalidade. 8. Em se tratando de compartilhamento das informações do consumidor pelos bancos de dados, prática essa autorizada pela Lei 12.414/2011 em seus arts. 4º, III, e 9º, deve ser observado o disposto no art. 5º, V, da Lei 12.414/2011, o qual prevê o direito do cadastrado ser informado previamente sobre a identidade do gestor e sobre o armazenamento e o objetivo do tratamento dos dados pessoais. 9. O fato, por si só, de se tratarem de dados usualmente fornecidos pelos próprios consumidores quando da realização de qualquer compra no comércio, não afasta a responsabilidade do gestor do banco de dados, na medida em que, quando o consumidor o faz não está, implícita e automaticamente, autorizando o comerciante a divulgá-los no mercado; está apenas cumprindo as condições necessárias à concretização do respectivo negócio jurídico entabulado apenas entre as duas partes, confiando ao fornecedor a proteção de suas informações pessoais. 10. Do mesmo modo, o fato de alguém publicar em rede social uma informação de caráter pessoal não implica o consentimento, aos usuários que acessam o conteúdo, de utilização de seus dados para qualquer outra finalidade, ainda mais com fins lucrativos. 11. Hipótese em que se configura o dano moral in re ipsa. 12. Em virtude do exame do mérito, por meio do qual foram rejeitadas as teses sustentadas pela recorrente, fica prejudicada a análise da divergência jurisprudencial. 13. Recurso especial conhecido em parte e, nessa extensão, desprovido. **(Grifo nosso)**<sup>71</sup>

É preciso, entretanto, entender como Direito de Acesso deve ser garantido a fim de possibilitar a real aplicação de outros direitos previstos na LGPD. Para tanto, utiliza-se como base de estudo indicações feitas por Stefano Rodotà sobre a dificuldade de efetividade do direito de Acesso aos dados pessoais, apresentadas por Carlos Edison do Rêgo Monteiro Filho e Diana Paiva de Castro (2019, p. 327), quais sejam:

(i) o aspecto do procedimento de acesso, relativo aos custos financeiros e de tempo envolvidos, à carência de alfabetização, à falta de informação e ao desnível de poder entre os titulares dos dados pessoais e os agentes públicos e privados que detêm as informações; (ii) o aspecto do funcionamento do acesso, que diz com a escassa relevância das informações fornecidas quando não se conhece o modo de funcionamento do sistema de tratamento e (iii) o aspecto do âmbito de incidência do acesso, referente ao excesso de vedações de acesso a certas categorias de informações.<sup>72</sup>

<sup>71</sup> STJ - REsp: 1758799 MG 2017/0006521-9, Relator: Ministra NANCY ANDRIGHI, Data de Julgamento: 12/11/2019, T3 - TERCEIRA TURMA, Data de Publicação: DJe 19/11/2019).

<sup>72</sup> MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

### 3.1 Procedimento de acesso

#### 3.1.1 O custo do acesso

Em países com grande desigualdade social, os custos atrelados à garantia do acesso aos dados são um problema a ser levado em conta. Exigir do titular uma compensação financeira pela disponibilização a este de informações que lhe dizem respeito seria acentuar o desequilíbrio de informações, pois além de desestimular o intento de controle, também geraria a exclusão de grande parte da sociedade na participação do controle de seus dados por entidades públicas e privadas.

Por isso, trouxe a LGPD, a disposição de que a consulta aos dados deverá ser gratuita, conforme descrito no princípio do livre acesso<sup>73</sup>. Além disso, prevê também o § 5º do artigo 18, que o requerimento de acesso deverá ser atendido sem custos para o titular.

Nota-se que a gratuidade do acesso se fazia necessária, já que qualquer cobrança em relação a essa prestação de informações poderia ser considerada injusta, já que, os dados pessoais dos titulares são recursos financeiros nas mãos dos interessados. Cobrar do titular pelo atendimento de uma informação que lhe é de direito a qual, em grande parte das vezes, ele não recebe retorno pelo fornecimento dos dados seria, desproporcional.

Há que se destacar que a LGPD é mais protetiva ao indivíduo nessa questão que o GDPR, já que este prevê a gratuidade de uma primeira cópia dos dados, mas a cobrança em outras que se sigam, conforme se depreende do número 3 do artigo 15:

“3. O responsável pelo tratamento fornece uma cópia dos dados pessoais em fase de tratamento. Para fornecer outras cópias solicitadas pelo titular dos dados, o responsável pelo tratamento pode exigir o pagamento de uma taxa razoável tendo em conta os custos administrativos. Se o titular dos dados apresentar o pedido por meios eletrônicos, e salvo pedido em contrário do titular dos dados, a informação é fornecida num formato eletrônico de uso corrente.”

---

<sup>73</sup> Art. 6º, IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;



Nesse sentido, o GDPR também prevê no parágrafo 5 do artigo 12 o pagamento pelo titular para o acesso aos dados, e até o seu não atendimento, quando os pedidos forem “*manifestamente infundados ou excessivos, nomeadamente devido ao seu caráter repetitivo*”.

A previsão da gratuidade acaba por ser um desafio às empresas e demais interessados no tratamento dos dados pessoais, pois não terão um subsídio para implementar e garantir esse acesso aos titulares. Entretanto, entende-se que dado o contexto brasileiro quanto às vulnerabilidades econômicas, a medida apresenta-se como uma proteção necessária.

### **3.1.2 A complexidade do acesso**

Era necessário também, considerar a falta de conhecimento do titular quanto à linguagem que envolve as atividades de processamento e do que significa cada aspecto do sistema de tratamento utilizado pelos controladores e operadores. A maioria dos titulares de dados é considerada leiga nesses assuntos e não conseguiria compreender um documento que não levasse a qualquer conclusão do que de fato se tem sobre o indivíduo, do que é feito com tais informações, com quem elas são compartilhadas, quem participa do processo, e outros pontos de conhecimento relevante.

Por isso, garante a LGPD a consulta facilitada, como descrito no artigo 6º, IV. Também o artigo 9º prevê que as informações sejam disponibilizadas de forma clara, adequada e ostensiva. É a preocupação de que o direito de acesso possa realmente atender à expectativa do titular em saber o que acontece com seus dados através de resposta escrita de maneira inteligível a ele.

É preciso, então, um esforço por parte dos agentes de tratamento em “traduzir” os dados e as informações que eles envolvam e disponibilizá-los de maneira que possa ser compreendida pelo titular. É possível ainda entender que a lei busca incentivar que os agentes de tratamento já mantenham em seus registros os dados pessoais e as informações que o envolvem em formato favorável ao atendimento do direito de acesso do titular, como se pode interpretar do artigo 19, § 1º: “*Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso*”.

### 3.1.3 O formato da informação

O artigo 19, em seus incisos I e II, dispõe que haverá duas formas principais de se atender ao pedido de acesso feito pelo titular: o formato simplificado e a declaração clara e completa acerca dos dados. Tal distinção, infere-se, foi uma maneira de a lei dispor de uma via mais econômica ao agente de tratamento, que teria que dispensar menos trabalho e tempo para atender à solicitação do titular, como se pode observar também na determinação dos prazos para resposta.

Além disso, permite a LGPD que o requerente escolha o meio com que quer ser respondido quanto à solicitação de acesso aos dados, qual sejam, o meio digital ou físico, conforme artigo 19, § 2º: *“As informações e os dados poderão ser fornecidos, a critério do titular: I - por meio eletrônico, seguro e idôneo para esse fim; ou II - sob forma impressa”*.

O § 3º dispõe ainda de formato que *“permita a sua utilização subsequente, inclusive em outras operações de tratamento”*, visando a garantia do direito de portabilidade que pode ser exercido pelo titular posteriormente ao acesso.

Interessante observar que o GDPR traz a possibilidade de o requerente receber as informações de maneira oral, conforme o final do parágrafo 1 do artigo 12: *“Se o titular dos dados o solicitar, a informação pode ser prestada oralmente, desde que a identidade do titular seja comprovada por outros meios”*. A LGPD não tem previsão neste sentido.

### 3.1.4 O prazo para resposta

Dada a possibilidade de uma resposta em formato simplificado (leia-se, resumido) ou de resposta a partir de declaração completa e clara acerca dos dados, a LGPD formulou dois prazos diferentes para as diferentes respostas.

Para a resposta em formato simplificado, prevê a lei que deverá ser concedida de forma imediata. É como se o dispositivo previsse que os agentes de tratamento já tivessem uma cópia

disponível dos dados de cada titular pronta para ser acessada quase que automaticamente quando o este o desejasse<sup>74</sup>.

Já para a declaração clara e completa, que envolveria um detalhismo maior, a lei dispõe de um prazo de 15 dias para o atendimento da solicitação pelo titular. Entende-se tratar de operação que demande mais trabalho para ser executada, já que a lei não obriga o agente de tratamento a ter já pronta uma cópia com os dados nesse formato.

Vale destacar que, considerando os diferentes ramos de atividades e suas complexidades diversas, a lei prevê ainda que a ANPD poderá dispor prazos diferentes, independentes dos já citados, para as diferentes áreas do âmbito privado e público, conforme se observa no § 4º do artigo 19: *“A autoridade nacional poderá dispor de forma diferenciada acerca dos prazos previstos nos incisos I e II do caput deste artigo para os setores específicos”*.

Caberá, portanto, à autoridade realizar estudos de viabilidade a fim de emitir normativas no sentido de garantir prazos mais longos para setores que teriam maior dificuldade em apresentar essas informações.

O GDPR já dispõe de um prazo maior, de 1 mês, prorrogável por até 2 meses, *“quando for necessário, tendo em conta a complexidade do pedido e o número de pedidos”*, devendo o responsável pelo tratamento comunicar ao titular da prorrogação e dos motivos desta, conforme parágrafo 3 do artigo 12.

### **3.1.5 A tutela assistida para acesso aos dados**

A LGPD preocupa-se com a vulnerabilidade do titular ante os agentes de tratamento, pois ao titular falta poder e informação. Tais faltas levam a uma dificuldade de o indivíduo se

---

<sup>74</sup> O GDPR, por outro lado, parece ter raciocínio diferente quanto a isso, à medida que nas disposições sobre os motivos do regulamento (Considerandos), há a previsão de que *“(64) O responsável pelo tratamento deverá adotar todas as medidas razoáveis para verificar a identidade do titular dos dados que solicite o acesso, em especial no contexto de serviços e de identificadores por via eletrônica. Os responsáveis pelo tratamento não deverão conservar dados pessoais com a finalidade exclusiva de estar em condições de reagir a eventuais pedidos”*.

posicionar frente aos interessados em seus dados para obter as informações que deseja. É por isso que a lei prevê a possibilidade de assistência por profissional qualificado.

Um profissional que tem conhecimento técnico e jurídico pode auxiliar o titular na solicitação de informações por parte dos agentes de tratamento garantindo ao indivíduo uma comunicação mais especializada e possível resposta mais adequada por parte dos agentes de tratamento. Permite então, a lei que *“Os direitos previstos neste artigo serão exercidos mediante requerimento expresso do titular ou de representante legalmente constituído, a agente de tratamento”* no § 3º, do artigo 18.

Também há a possibilidade da tutela coletiva dos direitos dos titulares quanto ao acesso dos dados, conforme dispõe o artigo 22 da lei: *“A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva”*.

Sobre a importância dessa representação, Carlos Edison Monteiro Filho e Diana Paiva de Castro (2019, p. 330) lembram a lição de Stefano Rodotà:

Segundo Rodotà, trata-se de “reforçar a posição dos indivíduos, seja para tornar mais eficaz o acesso, seja para suprir, no limite do possível, o *gap* de poder entre estes e os ‘senhores da informação’”. Isso pode se dar por meio de um “acesso ‘assistido’ por especialistas” – viabilizando-se “não somente o conhecimento das informações pessoais referentes ao interessado, mas também os ‘critérios utilizados para os tratamentos automáticos’” –, ou mediante “o reconhecimento de um direito de acesso ‘integrado’ pela presença de um sujeito coletivo (sindicato, associação de direitos civis, associação de tutela dos consumidores, e assim por diante).<sup>75</sup>

### 3.2 Funcionamento do acesso

Como o direito de acesso visa garantir ao titular o controle de sus dados e a capacidade de participar ativamente do processo de decisão que se utiliza deles, é preciso que o titular

---

<sup>75</sup> RODOTÀ, Stefano. *A vida na sociedade de vigilância: privacidade hoje*. Rio de Janeiro: Renovar, 2008. p. 68. apud MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

entenda não só quais dados seus são tratados, mas também como são tratados, por quais agentes de tratamento, com que objetivo e com quem eles são comunicados.

É por este motivo que prevê a LGPD em seu artigo 9º que o direito de acesso do titular abrange não só os dados, como também as informações relacionadas ao tratamento deles:

Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:

- I - finalidade específica do tratamento;
- II - forma e duração do tratamento, observados os segredos comercial e industrial;
- III - identificação do controlador;
- IV - informações de contato do controlador;
- V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
- VI - responsabilidades dos agentes que realizarão o tratamento; e
- VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei.

Sem o conhecimento da totalidade do processo que envolve seus dados, não é possível ao indivíduo tomar decisões totalmente conscientes quanto ao controle de seus dados pessoais e seus direitos de dispor deles para o tratamento por agentes de tratamento.

Tal capacidade de entendimento do sistema está ligada também à garantia do indivíduo de não ter os dados utilizados em desfavor de sua pessoa, conforme o artigo 21 da lei, que dispõe que *“Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo”*.

É por isso que a LGPD traz como possibilidade ao titular a revisão das decisões automatizadas tomadas a partir do processamento de seus dados. O indivíduo passa a ter a condição de conhecer o retrato de sua personalidade projetada pelo processamento de seus dados através de práticas como o *profiling*<sup>76</sup>, tanto realizadas pelos agentes de tratamento.

---

<sup>76</sup> Sobre o *profiling*, fala Danilo Doneda que “Entre estas técnicas, está a elaboração de perfis de comportamento de uma pessoa a partir de informações que ela disponibiliza ou que são colhidas. Esta técnica, conhecida como *profiling*, pode ser aplicada a indivíduos, bem como estendida a grupos. Com ela, os dados pessoais são tratados com o auxílio de métodos estatísticos e de técnicas de inteligência artificial, com o fim de se obter uma “metainformação”, que consistiria numa síntese dos hábitos, preferências pessoais e outros registros da vida desta pessoa. O resultado pode ser utilizado para traçar um quadro das tendências de futuras decisões, comportamentos e destino de uma pessoa ou grupo. A técnica pode ter várias aplicações desde o controle de entrada de pessoas em um determinado país pela alfândega, que selecionaria para um exame acurado as pessoas as quais é atribuída maior possibilidade de realizar atos contra o interesse nacional, até para finalidades privadas como o envio seletivo de mensagens publicitárias de um produto apenas para seus potenciais compradores, entre inúmeras outras.

Como as decisões tomadas de forma automática pelos recursos informáticos podem desconsiderar particularidades relevantes do indivíduo ou chegar a conclusões que levem em conta características que um grupo, que o indivíduo em tese pertence, tem em comum, mas não se trata de um aspecto de sua personalidade, tais hipóteses podem levar a um tratamento discriminatório, ferindo o princípio do artigo 6º, IX : “*não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos*”.

Sobre a discriminação, importante a reflexão de Caitlin Mulholland (2018, p. 164):

Em relação ao princípio da não discriminação, fica vedada a utilização dos dados pessoais para fins discriminatórios ilícitos ou abusivos. O legislador, ao relacionar o uso discriminatório às qualidades de ilicitude e abusividade, parece reconhecer a possibilidade de tratamento distintivo, desde que lícito e não abusivo. Isto é, aparentemente, seria legítimo ao operador de dados realizar tratamentos de segregação, no sentido de diferenciação, sem que, com isso leve a consequências excludentes que poderiam ser consideradas ilícitas. Assim, por exemplo, seria legítimo a um operador de dados que esteja realizando a precificação de um serviço de seguros de automóveis, tratar de maneira diferenciada os dados de mulheres entre 35 e 45 anos e mães, com a finalidade de oferecimento de um valor que reflita os riscos de danos usualmente ocasionados ou sofridos por esse grupo determinado de pessoas. Ou seja, há a possibilidade de tratamentos discriminatórios de dados, desde que não se caracterizem pela ilicitude ou abusividade, o que será determinado segundo critérios definidos tanto pelas regras expressas de direito civil e penal, quanto por princípios como o da boa-fé objetiva.<sup>77</sup>

A lei trouxe, então, a capacidade do indivíduo de, tendo o conhecimento de tais decisões, pedir que sejam revistas de acordo com a realidade de sua vida. Tal disposição se apresenta no artigo 20 da lei:

Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade

---

Um perfil assim obtido pode se transformar numa verdadeira representação virtual da pessoa, e pode ser o seu único aspecto visível a outros sujeitos que com ela terão algum tipo de interação. Este perfil estaria, em diversas circunstâncias, fadado a confundir-se com a própria pessoa.

A partir do momento em que um perfil eletrônico é a única parte da personalidade de uma pessoa visível a outrem, as técnicas de previsão de padrões de comportamento podem levar a uma diminuição de sua esfera de liberdade, visto que vários entes com os quais ela se relaciona partem do pressuposto que ela adotaria um comportamento predefinido, tendo como consequência uma potencial diminuição de sua liberdade de escolha visto que muitas de suas possibilidades podem ser pré-formatadas em função destas ilações" em DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019. p. 151-152.

<sup>77</sup> MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais*, Vitória, v. 19, n. 3, set./dez. 2018. p. 164.

§ 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.

§ 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais.

O Direito de revisão, possibilitado pelo acesso do titular aos seus dados e os procedimentos que o utilizam garante, assim, a liberdade para o desenvolvimento da personalidade do titular.

Quanto à quais informações o titular deve ter acesso, dispõe o GDPR de forma parecida, porém talvez de maneira um pouco mais específica, como se pode observar no parágrafo 1 do artigo 15:

1. O titular dos dados tem o direito de obter do responsável pelo tratamento a confirmação de que os dados pessoais que lhe digam respeito são ou não objeto de tratamento e, se for esse o caso, o direito de aceder aos seus dados pessoais e às seguintes informações:

- a) As finalidades do tratamento dos dados;
- b) As categorias dos dados pessoais em questão;
- c) Os destinatários ou categorias de destinatários a quem os dados pessoais foram ou serão divulgados, nomeadamente os destinatários estabelecidos em países terceiros ou pertencentes a organizações internacionais;
- d) Se for possível, o prazo previsto de conservação dos dados pessoais, ou, se não for possível, os critérios usados para fixar esse prazo;
- e) A existência do direito de solicitar ao responsável pelo tratamento a retificação, o apagamento ou a limitação do tratamento dos dados pessoais no que diz respeito ao titular dos dados, ou do direito de se opor a esse tratamento;
- f) O direito de apresentar reclamação a uma autoridade de controlo;
- g) Se os dados não tiverem sido recolhidos junto do titular, as informações disponíveis sobre a origem desses dados;
- h) A existência de decisões automatizadas, incluindo a definição de perfis, referida no artigo 22.º, n.ºs 1 e 4, e, pelo menos nesses casos, informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados.

Além da revisão das decisões automatizadas, através do conhecimento dos dados pessoais tratados e de como funciona tal tratamento, poderá o titular exercer os demais direitos previstos no artigo 18, citado anteriormente, bem como outros dispersos em demais dispositivos da lei.

### 3.3 Incidência do acesso

A LGPD veio sistematizar a tutela dos dados pessoais tratados em âmbito público e privado, como dispõe seu artigo 1º:

Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Assim, os direitos que ela prevê devem ser observados por todos os que mantenham as relações de tratamentos de dados pela lei tutelados, como observam Carlos Edison Monteiro Filho e Diana Paiva de Castro (2019, p. 338):

Exige-se, (...) que o direito de acesso possa ser exercido em face da sociedade, do mercado e também do Estado, isto é, sem que existam searas sociais em que prevaleça o sigilo em vez do controle. Por essa razão, a nova legislação contempla, logo em seu artigo 1º, sua incidência para o tratamento realizado “por pessoa natural ou por pessoa jurídica de direito público ou privado”. O tema das operações de dados pessoais levadas a cabo pelo Poder Público é ainda objeto de capítulo específico (Capítulo IV), no qual se demanda que o Estado forneça informações claras e atualizadas, em veículos de fácil acesso, preferencialmente nos *sites* oficiais, sobre os tratamentos de dados pessoais que efetua, sobretudo no que tange à previsão legal, à finalidade, aos procedimentos e às práticas utilizadas para a execução dessas operações (art. 23, I). Com efeito, o direito à privacidade deve ser tutelado em toda e qualquer relação intersubjetiva, tanto em face de agentes particulares quanto de agentes públicos (eficácia horizontal e vertical do direito fundamental ao controle dos dados pessoais). Afasta-se, assim, a concepção do estudo do direito por setores pré-constituídos, tendo como premissa básica a superação das divisões estanques entre as disciplinas jurídicas envolvidas (direito civil, administrativo, constitucional e processo civil), ou seja, uma visão unitária do ordenamento, e, especialmente, o rompimento dos lindes entre o público e o privado.<sup>78</sup>

Garantindo o acesso à integralidade dos dados<sup>79</sup>, isto é, a todos os dados pessoais que são tratados por pessoas públicas ou privadas, a lei tutela o protagonismo do titular no controle de seus dados. Estimula assim, a superação de controle excessivo sobre as pessoas por parte das entidades que era realizado através de muitas vedações ao acesso, preservando a dignidade humana através da importância dada à informação e o controle do titular ante ao sigilo.

<sup>78</sup> MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 338.

<sup>79</sup> “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”



### 3.4 As dificuldades do direito de acesso e a atuação da ANPD

As principais dificuldades em se garantir a efetividade do direito de acesso se dão principalmente em relação às limitações dos segredos comercial e industrial. A lei dispõe desta forma a fim de proteger a atividade econômica e as técnicas de processamento de dados que são desenvolvidas no interior dos agentes de tratamento, que não deixam de ser propriedades intelectuais desses agentes.

Entretanto, tal proteção da propriedade dos interessados no tratamento não pode ser utilizada de forma a diminuir o direito dos titulares, conforme observam Newton De Lucca e Renata Maciel (2020, p. 225):

Embora o dispositivo tente franquear ao titular dos dados o acesso facilitado às informações sobre o tratamento de seus dados, há o risco de que a ressalva, constante do inciso II, quanto ao segredo comercial e industrial - a qual, obviamente, é adequada e atende ao desenvolvimento da atividade empresarial - possa ser utilizada de forma abusiva, Impedindo o acesso do titular dos dados a essas informações.<sup>80</sup>

Nesse sentido, interessante o Considerando 63 do GDPR, que dispõe da proteção ao direito de autor do software, mas que ressalta que tal direito não deve ser desculpa para o não cumprimento do direito de acesso do titular:

(63) Os titulares de dados deverão ter o direito de aceder aos dados pessoais recolhidos que lhes digam respeito e de exercer esse direito com facilidade e a intervalos razoáveis, a fim de conhecer e verificar a tomar conhecimento do tratamento e verificar a sua licitude. Aqui se inclui o seu direito de acederem a dados sobre a sua saúde, por exemplo os dados dos registos médicos com informações como diagnósticos, resultados de exames, avaliações dos médicos e quaisquer intervenções ou tratamentos realizados. Por conseguinte, cada titular de dados deverá ter o direito de conhecer e ser informado, nomeadamente, das finalidades para as quais os dados pessoais são tratados, quando possível do período durante o qual os dados são tratados, da identidade dos destinatários dos dados pessoais, da lógica subjacente ao eventual tratamento automático dos dados pessoais e, pelo menos quando tiver por base a definição de perfis, das suas consequências. Quando possível, o responsável pelo tratamento deverá poder facultar o acesso a um sistema seguro por via eletrónica que possibilite ao titular aceder diretamente aos seus dados pessoais. **Esse direito não deverá prejudicar os direitos ou as liberdades de terceiros, incluindo o segredo comercial ou a propriedade intelectual e, particularmente, o direito de autor que protege o software. Todavia, essas considerações não deverão resultar na recusa de prestação de todas as informações ao titular dos dados.** Quando o responsável proceder ao tratamento de grande quantidade de informação relativa ao titular dos dados, deverá poder solicitar que, antes de a informação ser fornecida, o titular

<sup>80</sup> DE LUCCA, Newton; MACIEL, Renata Mota. A Proteção de Dados Pessoais no Brasil a partir da Lei 13.709/2018: Efetividade?, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). *Direito Digital – Direito Privado e Internet*. 3.ed. Indaiatuba, SP: Editora Foco, 2020. p. 225.

especifique a que informações ou a que atividades de tratamento se refere o seu pedido. (Grifo nosso)

Ademais, é necessário se assegurar que o segredo comercial e industrial não será utilizado de forma a preservar tratamentos discriminatórios entre os titulares de dados pessoais.

Por isso, é de vital importância o papel a ser desempenhado pela Autoridade Nacional de Proteção de Dados na garantia do direito de acesso aos dados, e consequentemente nos demais direitos do titular. A LGPD dispõe, portanto, no artigo 51 que *“A autoridade nacional estimulará a adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais”*.

A ANPD, que foi criada pela MP 869/18<sup>81</sup>, e que começa a ter sua estrutura formada, tem suas competências descritas no artigo 55-J da LGPD:

Art. 55-J. Compete à ANPD:

- I - zelar pela proteção dos dados pessoais, nos termos da legislação;
- II - **zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;**
- III - **elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;**
- IV - **fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;**
- V - **apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;**
- VI - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

<sup>81</sup> Sobre a criação da ANPD: “Assinale se que o Poder Executivo editou, no dia 28/12/2018, a Medida Provisória 869/2018, que alterou a LGPD, de 14 de agosto de 2018, dispondo sobre a proteção de dados pessoais, criando a Autoridade Nacional de Proteção de Dados e dando outras providências. Foi a última medida importante tomada pelo então presidente Michel Temer, que houvera estabelecido o veto, não por ser contrário a criação da referida Autoridade Nacional de Proteção de Dados por ele tida como necessária, mas em razão de ser competência do Poder Executivo, e não do Legislativo, a criação de órgão. As razões do veto presidencial relativas a esse ponto específico foram: “Os dispositivos incorrem em inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, ‘e’, cumulado com o artigo 37, XIX da Constituição”. Tais dispositivos estabelecem, de um lado, ser de competência privativa do Presidente da República a iniciativa de leis que disponham sobre “criação, estruturação e atribuições dos Ministérios e órgãos da administração pública” (artigo 61, § 1º, II, ‘e’) e, de outro, que “somente por lei específica poderão ser criadas “empresa pública, sociedade de economia mista, autarquia e fundação pública” (artigo 37, XIX). Ainda que a cumulação referida nas razões do veto com esse art. 37, XIX, pudesse ser questionada, já que se tratava, no caso, de “lei específica”, o fato é que a aplicação do artigo 61, § 1º, II, alínea ‘e’, é absolutamente incontroversa, não tendo o Congresso Nacional tentado derrubar o veto do Presidente da República.” DE LUCCA, Newton, MACIEL, Renata Mota, A Lei n. 13.709, de 14 de agosto de 2018: a disciplina normativa que falava. In DELUCCA, Newton, SIMÃO FILHO, Adalberto; LIMA, Cintia Rosa Pereira de; MACIEL, Renata Meta (Conds). *Direito Internet IV: sistema de proteção de dados pessoais*. São Paulo: Quartier Latin, 2019. p. 37-38.

VII - promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

**VIII - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis;**

IX - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional;

**X - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial;**

**XI - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei;**

XII - elaborar relatórios de gestão anuais acerca de suas atividades;

**XIII - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;**

XIV - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento;

XV - arrecadar e aplicar suas receitas e publicar, no relatório de gestão a que se refere o inciso XII do caput deste artigo, o detalhamento de suas receitas e despesas;

XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;

XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942;

**XVIII - editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei;**

**XIX - garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003 (Estatuto do Idoso);**

XX - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos;

XXI - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento;

XXII - comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal;

XXIII - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e

XXIV - implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei.

§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei.

§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.

§ 3º A ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com a maior eficiência e promover o adequado funcionamento dos setores regulados, conforme legislação específica, e o tratamento de dados pessoais, na forma desta Lei.

§ 4º A ANPD manterá fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública responsáveis pela regulação de setores específicos da atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

**§ 5º No exercício das competências de que trata o caput deste artigo, a autoridade competente deverá zelar pela preservação do segredo empresarial e do sigilo das informações, nos termos da lei.**

§ 6º As reclamações colhidas conforme o disposto no inciso V do caput deste artigo poderão ser analisadas de forma agregada, e as eventuais providências delas decorrentes poderão ser adotadas de forma padronizada. **(Grifos nossos)**

Assim, caberá à ANPD a normatização quanto a especificidades da aplicação das disposições da Lei Geral de Proteção de Dados.

Para garantir o direito de Acesso, ela precisará, portanto, emitir normas referentes à forma como os dados deverão ser comunicados ao titular, levando a maior proteção à capacidade dele de controlar seus próprios dados (inclusive de modo a serem entendidos por pessoas de mais idade, como descreve o inciso XIX do artigo 55-J), bem como a uma maior segurança jurídica do atendimento a esse direito pelos agentes de tratamento. Regular o formato simplificado e a declaração completa de forma mais minuciosa, pode ser um grande serviço da ANPD à garantia dos direitos da proteção de dados.

Além disso, regulamentar os prazos de atendimento que não sejam os dispostos no art. 19, § 4º, para setores específicos poderá garantir que os agentes de tratamento consigam atender as demandas de acesso pelos titulares conforme a capacidade técnica e econômica destes, preservando o desenvolvimento econômico e a segurança jurídica.

Por fim, será de grande acréscimo a atuação da ANPD como fiscalizadora das atividades de tratamento, podendo realizar auditorias e recebendo as reclamações dos titulares. Esta atividade de fiscalização poderá garantir efetividade ao sistema de proteção de dados dos indivíduos proposto pela LGPD, conforme ressaltam Laura Mendes e Danilo Doneda (2018, p. 27):

a Autoridade é elemento indispensável para que os direitos e garantias dos cidadãos sobre seus dados sejam efetivamente implementados e monitorados. Além de a Autoridade ser um ponto de referência e orientação para o cidadão, ocorre que o

tratamento de dados pessoais é uma atividade complexa e que muitas vezes acontece de forma opaca, sendo realizado por entidades e corporações cujas práticas não são suficientemente transparentes – e que podem ser abusivas. A existência de uma Autoridade que atue de forma coordenada para prevenir e reprimir abusos, fiscalizando e tutelando tratamentos de dados de inteiras coletividades é fundamental para diminuir a distância abissal entre o cidadão e os entes que tratam seus dados, evitando que sejam abertas demandas individuais pelo caminho geralmente longo (e custoso) da via judicial.<sup>82</sup>

---

<sup>82</sup> MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): O novo paradigma da proteção de dados no Brasil. *Revista de Direito do Consumidor*, v. 120, p. 555-587, nov./dez. 2018.

## CONCLUSÃO

No contexto da sociedade da informação, o processamento de dados pessoais permeia grande parte das relações sociais entre as pessoas e as mais diversas entidades públicas e privadas. O processamento de dados pode, entretanto, levar a um risco para o indivíduo quando é feito com finalidades de controle, bem como quando retira do indivíduo a sua capacidade de determinar sua identidade no meio público.

Entendendo esse risco, a decisão do tribunal alemão no caso da lei do recenseamento em 1983 foi crucial para o desenvolvimento da privacidade através dos direitos à dignidade humana e ao livre desenvolvimento da personalidade. A fundamentação do direito a autodeterminação informativa no julgamento se mostrou grande aliada à proteção dos indivíduos e das projeções de sua personalidade através dos dados.

As leis que envolviam o processamento de dados pessoais foram se desenvolvendo a partir de uma regulação inicialmente voltada para os procedimentos utilizados pelos bancos de dados para uma proteção mais focada na dignidade humana e na capacidade do indivíduo de controlar os seus dados pessoais, levando em consideração que tal tratamento é necessário e essencial às atividades dos agentes econômicas e às atividades administrativas do Estado.

No Brasil, a tutela dos dados pessoais era realizada de forma dispersa em vários dispositivos com objetivos mais específicos. Assim, já havia instrumentos como o *habeas data*, que tutelavam o direito de acesso e retificação de informações pessoais sob a posse de bancos públicos; as disposições do Código de Defesa do Consumidor acerca dos bancos de dados com informações de consumo; a Lei do Cadastro Positivo que visava incluir informações de adimplemento (positivas) acerca dos indivíduos em bancos de dados voltados à concessão de crédito; bem como a Lei de Acesso a informação, que presava pela transparência dos órgãos públicos na divulgação de informações aos cidadãos.

A Lei Geral de Proteção de Dados veio para suprir a demanda de uma normativa específica que regulasse as atividades de tratamento de dados, ditando conceitos e padronizando o direito à proteção de dados no Brasil. A proteção conferida pelos diplomas anteriores não deixa de valer, sendo necessária, na verdade, sua aplicação conjunta aos casos específicos.

Entre os direitos conferidos pela LGPD, o Direito de Acesso apresenta especial relevância para a garantia de outros direitos que dele derivam e também são dispostos na lei. O direito de acessar os dados pessoais processados pelas entidades que figuram como agentes de tratamento, possibilita, por exemplo, que o indivíduo perceba um erro em seus dados e possa corrigi-lo, bem como que possa cancelar todo o tratamento revogando seu consentimento, por exemplo. É através dele que o indivíduo tem a possibilidade de controlar seus dados e se desenvolver como pessoa.

Há, entretanto, dificuldades relacionadas à efetividade de tal direito que envolvem aspectos de como ele funcionaria na prática de forma a garantir que o titular seja de fato informado sobre o que é feito com seus dados e possa tomar decisões quanto a essas informações.

Objetivando garantir a tutela desse direito, a LGPD traz disposições acerca do prazo e da forma como esses dados devem ser comunicados, bem como da necessidade de que eles sejam transmitidos de maneira inteligível aos titulares. Prevê também a possibilidade de que os titulares sejam representados ante os agentes de tratamento, para que a vulnerabilidade daqueles seja um pouco suprimida. Além disso, garante que o indivíduo precisa entender o processo de tratamento de seus dados para compreender onde eles se colocam nas finalidades dos interessados no tratamento, permitindo que ao visualizar eventuais discriminações, o titular possa se opor e solicitar a revisão de decisões automatizadas.

Portanto, prevendo a LGPD condições que facilitem a manutenção do direito de acesso aos dados, trouxe bastante avanço na tutela dos dados pessoais e na capacidade dos indivíduos de controlar seus dados. Porém, ainda que a lei disponha que o acesso deve ser garantido à integralidade dos dados pessoais, isto é, dos agentes de tratamento públicos e privados, restam algumas especificidades a serem resolvidas.

Nesse âmbito, tem muito a contribuir para a tutela do direito de Acesso e dos demais direitos relacionados à proteção de dados a Autoridade Nacional de Proteção de Dados recém constituída. Em suas disposições acerca de prazos, de regulações mais minuciosas sobre do atendimento às solicitações dos titulares e na atuação como fiscal da lei nos casos específicos através do recebimento de reclamações e da aplicação de sanções, a ANPD poderá garantir efetividade ao Direito de Acesso, e aos demais direitos previstos na LGPD.

## REFERÊNCIAS

BARCELLOS, Daniela Silva Fontoura; BARCELLOS, Tatiana Silva Fontoura. O Cadastro Positivo no Brasil: Uma análise empírica a partir dos casos julgados do Superior Tribunal De Justiça. **Revista de Direito, Economia e Desenvolvimento Sustentável**. v. 3, n.1, p. 52-73. Brasília, jan./jun. 2017.

BIONI, Bruno. **Proteção de Dados Pessoais – A Função e os Limites do Consentimento**. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. Código de Defesa do Consumidor. **Lei n. 8.078, de 11 de setembro de 1990**. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 10 jan. 2007.

\_\_\_\_\_. Constituição (1988). **Constituição da República Federativa do Brasil**. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 5 out. 1941.

\_\_\_\_\_. Lei de Acesso à Informação. **Lei n. 12.527, de 18 de novembro de 2011**. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 18 nov. 2011.

\_\_\_\_\_. Lei do Cadastro Positivo. **Lei n. 12.414, de 9 de junho de 2011**. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 10 jun. 2011.

\_\_\_\_\_. Lei Geral de Proteção de Dados (LGPD). **Lei n. 13.709, de 14 de agosto de 2018**. Diário Oficial [da] República Federativa do Brasil, Poder Executivo, Brasília, DF, 15 ago. 2018.

\_\_\_\_\_, Superior Tribunal de Justiça. Recurso Especial nº 22.337/RS, rel. Ministro Ruy Rosado de Aguiar, DJ 20/03/1995.

\_\_\_\_\_, Superior Tribunal de Justiça. Recurso Especial nº 1.758.799/MG 2017/0006521-9, rel. Ministra Nancy Andrighi, DJe 19/11/2019.

\_\_\_\_\_, Superior Tribunal Federal. Recurso Extraordinário nº 673.707/MG, rel. Ministro Luiz Fux, DJe 17/06/2017.



BRITZ, Gabriele. Freie **Entfaltung durch Selbstdarstellung**. Tübingen: Mohr Siebeck, 2007. apud MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

**BVerfGE 65, 1, Volkszählung** (Recenseamento), 1983. apud MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

CASTRO, Catarina Sarmiento. Os ficheiros de crédito e a protecção de dados pessoais. **Boletim da Faculdade de Direito**, Coimbra, v. LXXVII, 2002. apud LAEBER, Márcio Rafael Silva. Proteção de Dados Pessoais: O Direito à Autodeterminação Informativa. *Revista de Direito Bancário e do Mercado de Capitais*, v. 37, p. 59-80, jul-set 2007.

DONEDA, Danilo. **Da privacidade à proteção dos dados pessoais**. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

\_\_\_\_\_. O Direito Fundamental à Proteção de Dados Pessoais, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). **Direito Digital – Direito Privado e Internet**. 3.ed. Indaiatuba, SP: Editora Foco, 2020.

DE LUCCA, Newton, MACIEL, Renata Mota, A Lei n. 13.709, de 14 de agosto de 2018: a disciplina normativa que falava. In DELUCCA, Newton, SIMÃO FILHO, Adalberto; LIMA, Cinta Rosa Pereira de: MACIEL, Renata Meta (Coord.). **Direito Internet IV: sistema de proteção de dados pessoais**. São Paulo: Quartier Latin, 2019.

\_\_\_\_\_. A Proteção de Dados Pessoais no Brasil a partir da Lei 13.709/2018: Efetividade?, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). **Direito Digital – Direito Privado e Internet**. 3.ed. Indaiatuba, SP: Editora Foco, 2020.

EDELMAN, Bernard. **La personne en danger**. Paris: Puf, 1999. p. 377. apud DONEDA, Danilo. *Da privacidade à proteção dos dados pessoais*. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

FROSINI, Vittorio. *Contributi ad un diritto dell'informazione*. Napoli: Liguori, 1991. apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

HIRATA, Alessandro. Direito à privacidade. Enciclopédia jurídica da PUC-SP. CAMPILONGO, Celso Fernandes; GONZAGA, Alvaro de Azevedo; FREIRE, André Luiz (Coord.). Tomo: Direito Administrativo e Constitucional. NUNES JUNIOR, Vidal Serrano; ZOCKUN, Maurício; ZOCKUN, Carolina Zancaner, FREIRE, André Luiz (Coord. de Tomo). 1. ed. São Paulo: Pontifícia Universidade Católica de São Paulo, 2017. Disponível em: <https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade> - Acesso em 29 de outubro de 2020.

HOFMANN, Hasso. La promessa della dignità umana. **Rivista Internazionale di Filosofia del Diritto**, IV serie. v. 76, p. 620-650, 1999, apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

HOFFMANN-RIEM, Wolfgang. **Grundrechts- und Funktionsschutz für elektronisch vernetzte Kommunikation**. Archiv des öffentlichen Rechts, 134, 2009. apud MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

KANT, Immanuel. **Fundamentos da metafísica do costume**. Tradução: Paulo Quintela. Lisboa: Edições 70, 2000.

LAEBER, Márcio Rafael Silva. Proteção de Dados Pessoais: O Direito à Autodeterminação Informativa. **Revista de Direito Bancário e do Mercado de Capitais**, v. 37, p. 59-80, jul-set 2007.

LIMBERGER, Têmis. Informação em Rede: Uma comparação da Lei Brasileira de Proteção de Dados Pessoais e o Regulamento Geral de Proteção de Dados Europeu, in: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti (Coord.). **Direito Digital – Direito Privado e Internet**. 3.ed. Indaiatuba, SP: Editora Foco, 2020.

LISBOA, Roberto Senise. Direito na sociedade da informação. **Revista dos Tribunais**, ano 95, v. 847, p. 78-95, mai 2006.

MATOS, Ana Carla Harmatiuk; RUZYK, Carlos Eduardo Pianovski. Diálogos entre a Lei Geral de Proteção de Dados e a Lei de Acesso à informação. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. Ed. São Paulo: Thomson Reuters Brasil, 2019.

MENDES, Laura Schertel Ferreira. *Habeas data* e autodeterminação informativa: os dois lados da mesma moeda. **Direitos Fundamentais & Justiça**, Belo Horizonte, ano 12, n. 39, p. 185-216, jul./dez. 2018.

MENDES, Laura Schertel; DONEDA, Danilo. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): O novo paradigma da proteção de dados no Brasil. **Revista de Direito do Consumidor**, v. 120, p. 555-587, nov./dez. 2018.

MIRAGEM, Bruno. A Lei Geral De Proteção De Dados (Lei 13.709/2018) e o Direito Do Consumidor. **Revista dos Tribunais**, v. 1009, p. 173 - 222, nov. 2019.

MIRANDA, Felipe Arady. O Direito Fundamental ao Livre Desenvolvimento da Personalidade. **Revista do Instituto do Direito Brasileiro**, Lisboa, ano 2, n. 10, p. 11175-11211, 2013.

MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

MULHOLLAND, Caitlin Sampaio. Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 19, n. 3, p. 159-180, set./dez. 2018.

PÉREZ LUÑO, Antonio-Enrique. Los derechos humanos en la sociedad tecnológica, in: LOSANO, Mario; PÉREZ LUÑO, Antonio-Enrique; GUERRERO MATEUS, Maria Fernanda. **Libertad informática y leyes de protección de datos personales**. Madrid: Centro de Estudios Constitucionales, 1989, p. 137-162. apud DONEDA, Danilo. Da privacidade à proteção dos dados pessoais. 2. Ed. São Paulo: Thomson Reuters Brasil, 2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008. apud MONTEIRO FILHO, Carlos Edison do Rêgo; CASTRO, Diana Paiva. Potencialidades do direito de acesso na nova Lei Geral de Proteção de Dados (Lei 13.709). In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019.

UNIÃO EUROPEIA. **Regulamento (UE) nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Jornal Oficial da União Europeia, Estrasburgo, 04/05/2016.